TIA/EIA INTERIM STANDARD

TIA/EIA/IS-856

cdma2000 High Rate Packet Data Air Interface Specification

TIA/EIA/IS-856

NOVEMBER 2000

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association represents the communications sector of

Electronic Industries Alliance

NOTICE

TIA/EIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards and Publications shall not in any respect preclude any member or nonmember of TIA/EIA from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than TIA/EIA members, whether the standard is to be used either domestically or internationally.

Standards and Publications are adopted by TIA/EIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA/EIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

TIA/EIA INTERIM STANDARDS

TIA/EIA Interim Standards contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of a TIA/EIA Standard.

TIA/EIA Interim Standards should be reviewed on an annual basis by the formulating Committee and a decision made on whether to proceed to develop a TIA/EIA Standard on this subject. TIA/EIA Interim Standards must be cancelled by the Committee and removed from the TIA/EIA Standards Catalog before the end of their third year of existence.

Publication of this TIA/EIA Interim Standard for trial use and comment has been approved by the Telecommunications Industry Association. Distribution of this TIA/EIA Interim Standard for comment shall not continue beyond 36 months from the date of publication. It is expected that following this 36 month period, this TIA/EIA Interim Standard, revised as necessary, will be submitted to the American National Standards Institute for approval as an American National Standard. Suggestions for revision should be directed to: Standards & Technology Department, Telecommunications Industry Association, 2500 Wilson Boulevard, Arlington, VA 22201.

(From Project No. 4875, formulated under the cognizance of the TIA TR-45.5 Subcommittee on Spread Spectrum Digital Technology.)

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 2000
Standards & Technology Department
2500 Wilson Boulevard
Arlington, VA 22201

PRICE: Please refer to current Catalog of
EIA ELECTRONIC INDUSTRIES ALLIANCE STANDARDS and ENGINEERING PUBLICATIONS or
call Global Engineering Documents, USA and Canada
(1-800-854-7179) International (303-397-7956)

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

FIGURES

FIGURES

FIGURES

FIGURES

TABLES

TABLES

TABLES

TABLES

FOREWORD

(This foreword is not part of this Standard)

This standard was prepared by Technical Specification Group C of the Third Generation Partnership Project 2 (3GPP2). This standard is evolved from and is a companion to the cdma2000 standards. This air interface standard provides high rate packet data services.

Ten different operating bands have been specified. Equipment built to this standard can be used in a band subject to the allocation of the band and to the rules and regulations of the country to which the allocated band has been assigned.

REFERENCES

The following standards contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[1] TIA/EIA/IS-835, Wireless IP Network Standard.

[2] TIA/EIA/IS-2000-2-A, Physical Layer Standard for cdma2000 Spread Spectrum Systems.

[3] TIA/EIA/IS-2000-5-A, Upper Layer (Layer 3) Signaling Specification for cdma2000 Spread Spectrum Systems.

[4] TIA/EIA/PN-4913, Recommended Minimum Performance Standards for cdma2000 High Rate Packet Data Access Network.

[5] TIA/EIA/PN-4916, Recommended Minimum Performance Standards for cdma2000 High Rate Packet Data Access Terminal.

[6] FIPS PUB 180-1, Federal Information Processing Standards Publication 180-1.

[7] RFC 2409, The Internet Key Exchange (IKE).

[8] RFC 1700, Assigned Numbers.

[9] TIA/EIA/IS-2001, Access Network Interfaces Technical Specification.

1 OVERVIEW

1.1 Scope of This Document

These technical requirements form a compatibility standard for cdma2000 high rate packet data systems. These requirements ensure that a compliant access terminal can obtain service through any access network conforming to this standard. These requirements do not address the quality or reliability of that service, nor do they cover equipment performance or measurement procedures.

This specification is primarily oriented toward requirements necessary for the design and implementation of access terminals. As a result, detailed procedures are specified for access terminals to ensure a uniform response to all access networks. Access network procedures, however, are specified only to the extent necessary for compatibility with those specified for the access terminal.

This specification includes provisions for future service additions and expansion of system capabilities. The architecture defined by this specification permits such expansion without the loss of backward compatibility to older access terminals.

This compatibility standard is based upon spectrum allocations that have been defined by various governmental administrations. Those wishing to deploy systems compliant with this standard should also take notice of the requirement to be compliant with the applicable rules and regulations of local administrations. Those wishing to deploy systems compliant with this standard should also take notice of the electromagnetic exposure criteria for the general public and for radio frequency carriers with low frequency amplitude modulation.

1.2 Requirements Language

Compatibility, as used in connection with this standard, is understood to mean: Any access terminal can obtain service through any access network conforming to this standard. Conversely, all access networks conforming to this standard can service access terminals.

"Shall" and "shall not" identify requirements to be followed strictly to conform to the standard and from which no deviation is permitted. "Should" and "should not" indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. "May" and "need not" indicate a course of action permissible within the limits of the standard. "Can" and "cannot" are used for statements of possibility and capability, whether material, physical, or causal.

1.3 Architecture Reference Model

The architecture reference model is presented in Figure 1.3-1. The reference model consists of the following functional units:

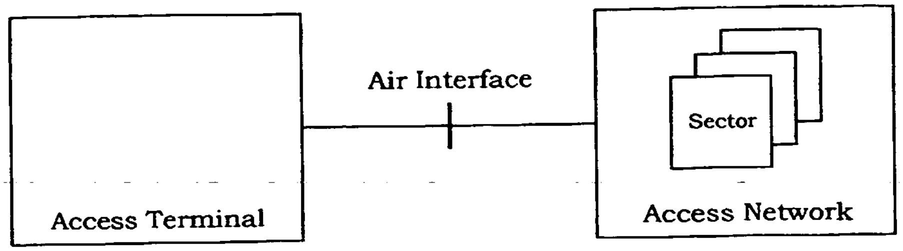


Figure 1.3-1. Architecture Reference Model

The access terminal, the access network, and the sector are formally defined in 1.11.

The reference model includes the air interface between the access terminal and the access network. The protocols used over the air interface are defined in this document.

1.4 Protocol Architecture

The air interface has been layered, with interfaces defined for each layer (and for each protocol within each layer). This allows future modifications to a layer or to a protocol to be isolated.

1.4.1 Layers

Figure 1.4.1-1 describes the layering architecture for the air interface. Each layer consists of one or more protocols that perform the layer's functionality. Each of these protocols can be individually negotiated.

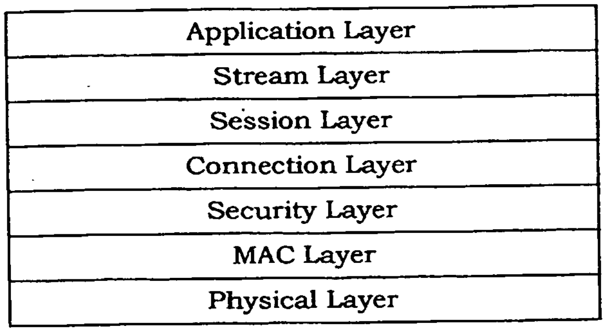


Figure 1.4.1-1. Air Interface Layering Architecture

The protocols and layers specified in Figure 1.4.1-1 are:

1. Application Layer: The Application Layer provides multiple applications. It provides the Default Signaling Application for transporting air interface protocol messages. The Default Signaling Application is defined in Chapter 2. It also provides the Default Packet Application for transporting user data. The Default Packet Application is defined in Chapter 3.

2. Stream Layer: The Stream Layer provides multiplexing of distinct application streams. Stream 0 is dedicated to signaling and defaults to the Default Signaling Application (see Chapter 2). Stream 1, Stream 2, and Stream 3 are not used by default. The Stream Layer is defined in Chapter 4.
3. Session Layer: The Session Layer provides address management, protocol negotiation, protocol configuration and state maintenance services. The Session Layer is defined in Chapter 5.
4. Connection Layer: The Connection Layer provides air link connection establishment and maintenance services. The Connection Layer is defined in Chapter 6.
5. Security Layer: The Security Layer provides authentication and encryption services. The Security Layer is defined in Chapter 7.
6. MAC Layer: The Medium Access Control (MAC) Layer defines the procedures used to receive and to transmit over the Physical Layer. The MAC Layer is defined in Chapter 8.
7. Physical Layer: The Physical Layer provides the channel structure, frequency, power output, modulation, and encoding specifications for the Forward and Reverse Channels. The Physical Layer is defined in Chapter 9.

Each layer may contain one or more protocols. Protocols use signaling messages or headers to convey information to their peer entity at the other side of the air-link. When protocols send messages they use the Signaling Network Protocol (SNP) to transmit these messages.

1.5 Physical Layer Channels

The Physical Layer defines the Physical Layer Channels and the Forward and Reverse Channel hierarchies shown in Figure 1.5-1 and Figure 1.5-2. Channel x is part of Channel y if y is an ancestor of x. The specific channels are defined in 1.11. When the context is clear, the complete qualified name is usually omitted (e.g., Pilot Channel as opposed to Forward Pilot Channel or Data Channel as opposed to Reverse Traffic Data Channel).

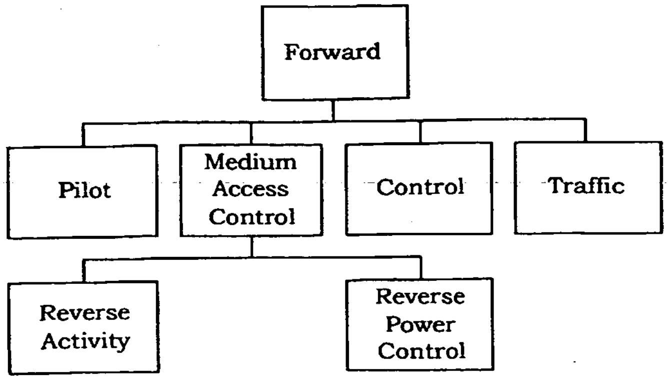


Figure 1.5-1. Forward Channel Structure

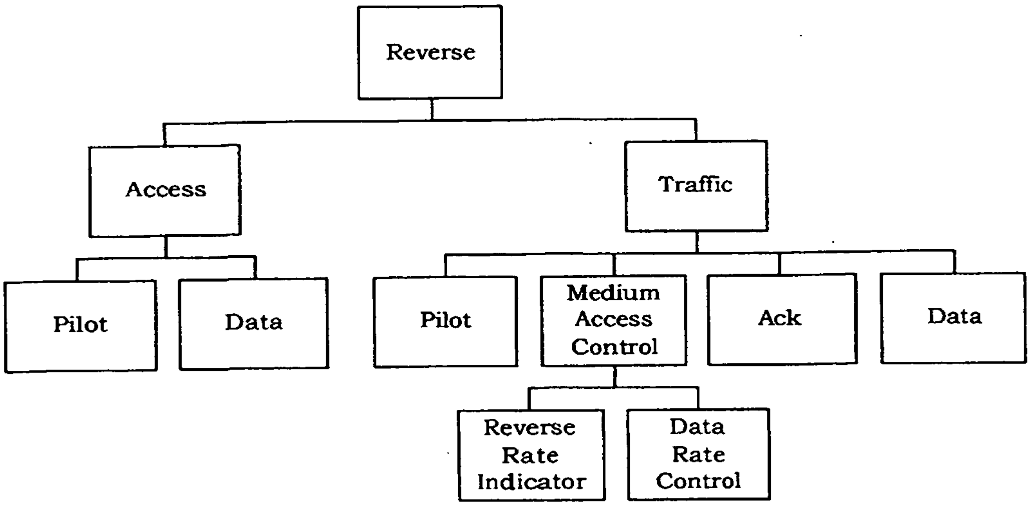


Figure 1.5-2. Reverse Channel Structure

1.6 Protocols

1.6.1 Interfaces

This standard defines a set of interfaces for communications between protocols in the same entity and between a protocol executing in one entity and the same protocol executing in the other entity.

In the following the generic term "entity" is used to refer to the access terminal and the access network.

Protocols in this specification have four types of interfaces:

- Headers and messages are used for communications between a protocol executing in one entity and the same protocol executing in the other entity.

- Commands are used by a higher layer protocol to obtain a service from a lower layer protocol in the same entity. Commands can be sent between protocols in the same layer but only in one direction (i.e., if protocol A and protocol B are in the same layer and protocol A sends a command to protocol B, protocol B cannot send a command to protocol A). For example, ***AccessChannelMAC.Abort*** causes the Access Channel MAC Protocol to abort any access attempt currently in progress.
- Indications are used by a lower layer protocol to convey information regarding the occurrence of an event. Any higher layer protocol can register to receive these indications. A same layer protocol can also register to receive an indication but only in one direction (if protocol A and protocol B are in the same layer and protocol A registers to receive an indication from protocol B, protocol B cannot register to receive an indication from protocol A.). For example, the access terminal Reverse Traffic Channel MAC Protocol returns a "Reverse Link Acquired" indication when it gets a message from its peer protocol at the access network that it has acquired the Reverse Traffic Channel. This notification is then used by Connection Layer protocols to continue with the handshake leading to the establishment of the connection.
- Public Data is used to share information in a controlled way between protocols. Public data is shared between protocols in the same layer, as well as between protocols in different layers. An example of this is the MinimumProtocolRevision made public by the Connection Layer Initialization State Protocol after the protocol receives it in the Sync message.

Commands and indications are written in the form of ***Protocol.Command*** and ***Protocol.Indication***. For example, ***AccessChannelMAC.Activate*** is a command activating the Access Channel MAC, and ***IdleState.ConnectionOpened*** is an indication provided by the Connection Layer Idle State Protocol that the connection is now open. When the context is clear, the ***Protocol*** part is dropped (e.g., within the Idle State Protocol, ***Activate*** refers to ***IdleState.Activate***).

Commands are always written in the imperative form, since they direct an action. Indications are always written in the past tense since they notify of events that happened (e.g., ***OpenConnection*** for a command and ***ConnectionOpened*** for an indication).

Headers and messages are binding on all implementations. Commands, indications, and public data are used as a device for a clear and precise specification. Access terminals and access networks can be compliant with this specification while choosing a different implementation that exhibits identical behavior.

1.6.2 States

When protocols exhibit different behavior as a function of the environment (e.g., if a connection is opened or not, if a session is opened or not, etc.), this behavior is captured in a set of states and the events leading to a transition between states.

Unless otherwise specifically mentioned, the state of the access network refers to the state of a protocol engine in the access network as it applies to a particular access terminal. Since the access network communicates with multiple access terminals, multiple independent instantiations of a protocol will exist in the access network, each with its own independent state machine.

Typical events leading to a transition from one state to another are the receipt of a message, a command from a higher layer protocol, an indication from a lower layer protocol, or the expiration of a timer.

When a protocol is not functional at a particular time (e.g., the Access Channel MAC protocol at the access terminal when the access terminal has an open connection) the protocol is placed in a state called the Inactive state. This state is common for most protocols.

Other common states are Open, indicating that the session or connection (as applicable to the protocol) is open and Close, indicating that the session or connection is closed.

If a protocol has a single state other than the Inactive state, that state is always called the Active state. If a protocol has more than one state other than the Inactive state, all of these states are considered active, and are given individual names (e.g., the Forward Traffic Channel MAC protocol has three states: Inactive, Variable Rate, and Fixed Rate).

1.6.3 Common Commands

Most protocols support the following two commands:

- ***Activate,*** which commands the protocol to transition away from the Inactive state to some other state.
- ***Deactivate,*** which commands the protocol to transition to the Inactive state. Some protocols do not transition immediately to the Inactive state, due to requirements on orderly cleanup procedures.

Other common commands are ***Open*** and ***Close,*** which command protocols to perform session open /close or connection open / close related functions.

1.6.4 Protocol Negotiation

Most protocols can be negotiated and can be configured when the session is set-up (see 1.9 for a discussion of sessions). Protocols are associated with a Type that denotes the type of the protocol (e.g., Access Channel MAC Protocol) and with a Subtype that denotes a specific instance of a protocol (e.g., the Default Access Channel MAC Protocol and perhaps one day, the Extended and Bloated Access Channel MAC Protocol).

The negotiation and configuration processes are part of the Session Layer.

1.6.5 Protocol Overview

Figure 1.6.5-1 presents the default protocols defined for each one of the layers shown in Figure 1.4.1-1. The following is a brief description of each protocol. A more complete description is provided in the Introduction section of each layer.

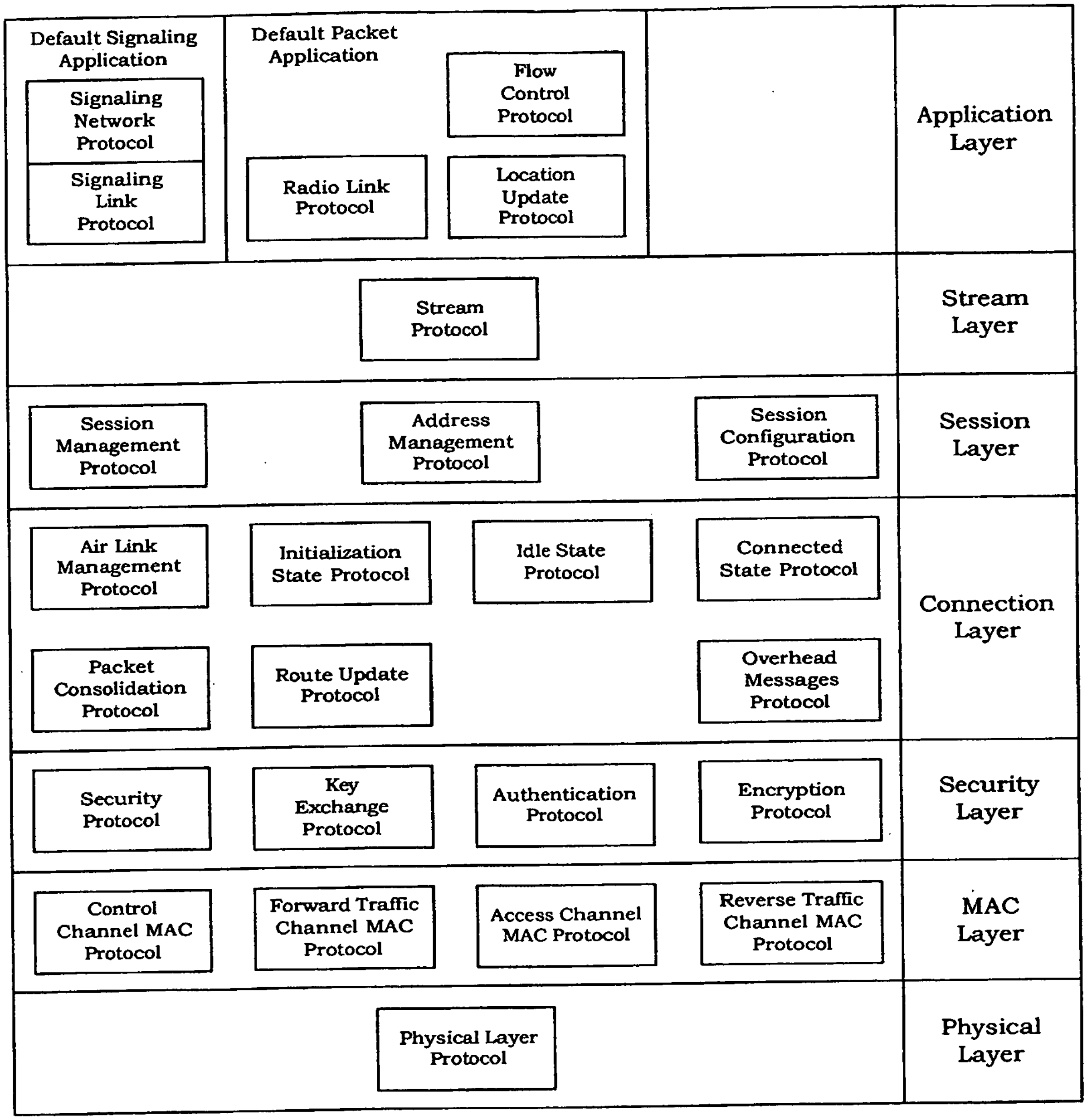

Default Signaling Application
Signaling Network Protocol
Signaling Link Protocol
Default Packet Application
Flow Control Protocol
Radio Link Protocol
Location Update Protocol
Application Layer
Stream Protocol
Stream Layer
Session Management Protocol
Address Management Protocol
Session Configuration Protocol
Session Layer
Air Link Management Protocol
Initialization State Protocol
Idle State Protocol
Connected State Protocol
Packet Consolidation Protocol
Route Update Protocol
Overhead Messages Protocol
Connection Layer
Security Protocol
Key Exchange Protocol
Authentication Protocol
Encryption Protocol
Security Layer
Control Channel MAC Protocol
Forward Traffic Channel MAC Protocol
Access Channel MAC Protocol
Reverse Traffic Channel MAC Protocol
MAC Layer
Physical Layer Protocol
Physical Layer

Figure 1.6.5-1. Default Protocols

- Application Layer:
  - Default Signaling Application:
    - + Signaling Network Protocol: The Signaling Network Protocol (SNP) provides message transmission services for signaling messages.
    - + Signaling Link Protocol: The Signaling Link Protocol (SLP) provides fragmentation mechanisms, along with reliable and best-effort delivery mechanisms for signaling messages. When used in the context of the Default Signaling Application, SLP carries SNP packets.
  - Default Packet Application:
    - + Radio Link Protocol: The Radio Link Protocol (RLP) provides retransmission and duplicate detection for an octet aligned data stream.
    - + Location Update Protocol: The Location Update Protocol defines location update procedures and messages in support of mobility management for the Default Packet Application.
    - + Flow Control Protocol: The Flow Control Protocol defines flow control procedures to enabling and disabling the Default Packet Application data flow.
- Stream Layer:
  - Stream Protocol: adds the stream header in the transmit direction; removes the stream header and forwards packets to the correct application on the receiving entity.
- Session Layer:
  - Session Management Protocol: provides means to control the activation and the deactivation of the Address Management Protocol and the Session Configuration Protocol. It also provides a session keep alive mechanism.
  - Address Management Protocol: Provides access terminal identifier (ATI) management.
  - Session Configuration Protocol: Provides negotiation and configuration of the protocols used in the session.
- Connection Layer:
  - Air Link Management Protocol: Provides the overall state machine management that an access terminal and an access network follow during a connection.
  - Initialization State Protocol: Provides the procedures that an access terminal follows to acquire a network and that an access network follows to support network acquisition.
  - Idle State Protocol: Provides the procedures that an access terminal and an access network follow when a connection is not open.

  - Connected State Protocol: Provides the procedures that an access terminal and an access network follow when a connection is open.
  - Route Update Protocol: Provides the means to maintain the route between the access terminal and the access network.
  - Overhead Messages Protocol: Provides broadcast messages containing information that is mostly used by Connection Layer protocols.
  - Packet Consolidation Protocol: Provides transmit prioritization and packet encapsulation for the Connection Layer.
- Security Layer:
  - Key Exchange Protocol: Provides the procedures followed by the access network and the access terminal to exchange security keys for authentication and encryption.
  - Authentication Protocol: Provides the procedures followed by the access network and the access terminal for authenticating traffic.
  - Encryption Protocol: Provides the procedures followed by the access network and the access terminal for encrypting traffic.
  - Security Protocol: Provides procedures for generation of a cryptosync that can be used by the Authentication Protocol and Encryption Protocol.
- MAC Layer:
  - Control Channel MAC Protocol: Provides the procedures followed by the access network to transmit, and by the access terminal to receive the Control Channel.
  - Access Channel MAC Protocol: Provides the procedures followed by the access terminal to transmit, and by the access network to receive the Access Channel.
  - Forward Traffic Channel MAC Protocol: Provides the procedures followed by the access network to transmit, and by the access terminal to receive the Forward Traffic Channel.
  - Reverse Traffic Channel MAC Protocol: Provides the procedures followed by the access terminal to transmit, and by the access network to receive the Reverse Traffic Channel.
- Physical Layer:
  - Physical Layer Protocol: Provides channel structure, frequency, power output and modulation specifications for the forward and reverse links.

1.7 Default Applications

This document defines two default applications that all compliant access terminals and access networks support:

- Default Signaling Application, which provides the means to carry messages between a protocol in one entity and the same protocol in the other entity. The Default Signaling Application consists of a messaging protocol (Signaling Network Protocol) and a link layer protocol that provides message fragmentation, retransmission and duplicate detection (Signaling Link Protocol).
- Default Packet Application. The Default Packet Application consists of a link layer protocol that provides octet retransmission and duplicate detection (Radio Link Protocol), a location update protocol that provides mobility between data service networks and a flow control protocol that provides flow control of data traffic.

The applications used and the streams upon which they operate are negotiated as part of session negotiation.

1.8 Streams

The air interface can support up to four parallel application streams. The first stream (Stream 0) always carries Signaling, and the other three can be used to carry applications with different Quality of Service (QoS) requirements or other applications.

1.9 Sessions and Connections

A session refers to a shared state between the access terminal and the access network. This shared state stores the protocols and protocol configurations that were negotiated and are used for communications between the access terminal and the access network.

Other than to open a session, an access terminal cannot communicate with an access network without having an open session.

A connection is a particular state of the air-link in which the access terminal is assigned a Forward Traffic Channel, a Reverse Traffic Channel and associated MAC Channels.

During a single session the access terminal and the access network can open and can close a connection multiple times.

1.10 Security

The air interface supports a security layer, which can be used for authentication and encryption of access terminal traffic transported by the Control Channel, the Access Channel, the Forward Traffic Channel and the Reverse Traffic Channel.

1.11 Terms

Access Network (AN).aThe network equipment providing data connectivity between packet switched data network (typically the Internet) and the access terminals. An access network is equivalent to a base station in [2].

Access Terminal (AT). A device providing data connectivity to a user. An access terminal may be connected to a computing device such as a laptop personal computer or it may be a self-contained data device such as a personal digital assistant. An access terminal is equivalent to a mobile station in [2].

ATI. Access Terminal Identifier.

BATI. Broadcast Access Terminal Identifier.

CDMA System Time in Slots. An integer value s such that: $s = \lfloor t \times 600 \rfloor$, where t represents CDMA System Time in seconds. Whenever the document refers to the CDMA System Time in slots, it is referring to the value s.

CDMA System Time. The time reference used by the system. CDMA System Time is synchronous to UTC time except for leap seconds and uses the same time origin as GPS time. Access terminals use the same CDMA System Time, offset by the propagation delay from the access network to the access terminal.

Channel. The set of channels transmitted between the access network and the access terminals within a given frequency assignment. A Channel consists of a Forward Link and a Reverse Link.

Connection Layer. The Connection Layer provides air link connection establishment and maintenance services. The Connection Layer is defined in Chapter 6.

Dedicated Resource. An access network resource required to provide any data service to the access terminal, e.g, Wireless IP Service (see [1]) that is granted to the access terminal only after access terminal authentication has completed successfully. Power control and rate control are not considered dedicated resources.

Forward Channel. The portion of the Channel consisting of those Physical Layer Channels transmitted from the access network to the access terminal.

Forward Control Channel. The channel that carries data to be received by all access terminals monitoring the Forward Channel.

Forward MAC Channel. The portion of the Forward Channel dedicated to Medium Access Control activities. The Forward MAC Channel consists of the RPC, and RA Channels.

Forward MAC Reverse Activity (RA) Channel. The portion of the Forward MAC Channel that indicates activity level on the Reverse Channel.

Forward MAC Reverse Power Control (RPC) Channel. The portion of the Forward MAC Channel that controls the power of the Reverse Channel for one particular access terminal.

Forward Pilot Channel. The portion of the Forward Channel that carries the pilot.

Forward Traffic Channel. The portion of the Forward Channel that carries information for a specific access terminal. The Forward Traffic Channel can be used as either Dedicated Resource or a non-Dedicated Resource. Prior to successful access terminal authentication, the Forward Traffic Channel serves as a non-Dedicated Resource. Only after successful access terminal authentication can the Forward Traffic Channel be used as a Dedicated Resource for the specific access terminal.

Frame. The duration of time specified by 16 slots or 26.66... ms.

Global Positioning System (GPS). A US government satellite system that provides location and time information to users. See Navstar GPS Space Segment/Navigation User Interfaces ICD-GPS-200 for specifications

I_{BATI}. Index to the ReceiveATIList identifying the ReceiveATIList structure corresponding to BATI.

$I_{currentUATI}$. Index to the ReceiveATIList identifying the ReceiveATIList structure corresponding to the current ATI.

$I_{newUATI}$. Index to the ReceiveATIList identifying the ReceiveATIList structure corresponding to newly received ATI.

I_{RATI}. Index to the ReceiveATIList identifying the ReceiveATIList structure corresponding to RATI.

MAC Layer. The MAC Layer defines the procedures used to receive and to transmit over the Physical Layer. The MAC Layer is defined in Chapter 8.

MATI. Multicast Access Terminal Identifier.

NULL. A value which is not in the specified range of the field.

Physical Layer. The Physical Layer provides the channel structure, frequency, power output, modulation, and encoding specifications for the forward and reverse links. The Physical Layer is defined in Chapter 9.

RATI. Random Access Terminal Identifier.

Reverse Access Channel. The portion of the Reverse Channel that is used by access terminals to communicate with the access network when they do not have a traffic channel assigned. There is a separate Reverse Access Channel for each sector of the access network.

Reverse Access Data Channel. The portion of the Access Channel that carries data.

Reverse Access Pilot Channel. The portion of the Access Channel that carries the pilot.

Reverse Channel. The portion of the Channel consisting of those Physical Layer Channels transmitted from the access terminal to the access network.

Reverse Traffic Ack Channel. The portion of the Reverse Traffic Channel that indicates the success or failure of the Forward Traffic Channel reception.

Reverse Traffic Channel. The portion of the Reverse Channel that carries information from a specific access terminal to the access network. The Reverse Traffic Channel can be used as either a Dedicated Resource or a non-Dedicated Resource. Prior to successful access terminal authentication, the Reverse Traffic Channel serves as a non-Dedicated Resource. Only after successful access terminal authentication can the Reverse Traffic Channel be used as a Dedicated Resource for the specific access terminal.

Reverse Traffic Data Channel. The portion of the Reverse Traffic Channel that carries user data.

Reverse Traffic MAC Channel. The portion of the Reverse Traffic Channel dedicated to Medium Access Control activities. The Reverse Traffic MAC Channel consists of the RRI and DRC Channels.

Reverse Traffic MAC Data Rate Control (DRC) Channel. The portion of the Reverse Traffic Channel that indicates the rate at which the access terminal can receive the Forward Traffic Channel.

Reverse Traffic MAC Reverse Rate Indicator (RRI) Channel. The portion of the Reverse Traffic Channel that indicates the rate of the Reverse Traffic Data Channel.

Reverse Traffic Pilot Channel. The portion of the Reverse Traffic Channel that carries the pilot.

RLP. Radio Link Protocol provides retransmission and duplicate detection for an octet-aligned data stream.

Sector. The part of the access network that provides one CDMA channel.

Security Layer. The Security Layer provides authentication and encryption services. The Security Layer is defined in Chapter 7.

Session Layer. The Session Layer provides protocol negotiation, protocol configuration, and state maintenance services. The Session Layer is defined in Chapter 5.

Slot. A duration of time specified by 1.66... ms.

SLP. Signaling Link Protocol provides best-effort and reliable-delivery mechanisms for signaling messages. SLP is defined in 2.4.

SNP. Signaling Network Protocol provides message transmission services for signaling messages. The protocols that control each layer use SNP to deliver their messages to their peer protocols.

Stream Layer. The Stream Layer provides multiplexing of distinct streams. Stream 0 is dedicated to signaling and defaults to the default signaling stream (SNP / SLP) and Stream 1 defaults to the default packet service (RLP). Stream 2 and Stream 3 are not used by default. The Stream Layer is defined in Chapter 4.

Subnet Mask (of length *n*). A 128-bit value whose binary representation consists of ***n*** consecutive '1's followed by 128-***n*** consecutive '0's.

UATI. Unicast Access Terminal Identifier.

Universal Coordinated Time (UTC). An internationally agreed-upon time scale maintained by the Bureau International de l'Heure (BIH) used as the time reference by nearly all commonly available time and frequency distribution systems.

UTC. Universal Temps Coordine. See Universal Coordinated Time.

1.12 Notation

A[i] The i^{th} element of array A. The first element of the array is A[0].

$<e_1, e_2, ..., e_n>$ A ***structure*** with elements 'e1', 'e2', ..., 'en'. Two structures E = $<e_1, e_2, ..., e_n>$ and F = $<f_1, f_2, ..., f_m>$ are equal iff 'm' is equal to 'n' and e_i is equal to f_i for i = 1, ...n. Given E = $<e_1, e_2, ..., e_n>$ and F = $<f_1, f_2, ..., f_m>$, the assignment "E = F" denotes the following set of assignments: $e_i = f_i$, for i = 1, ...n.

S.e The member of the structure 'S' that is identified by 'e'.

M[i:j] Bits i^{th} through j^{th} inclusive (i = j) of the binary representation of variable M. M[0:0] denotes the least significant bit of M.

| Concatenation operator. (A | B) denotes variable A concatenated with variable B.

× Indicates multiplication.

$\lfloor x \rfloor$ Indicates the largest integer less than or equal to x: $\lfloor 1.1 \rfloor = 1$, $\lfloor 1.0 \rfloor = 1$.

$\lceil x \rceil$ Indicates the smallest integer greater or equal to x: $\lceil 1.1 \rceil = 2$, $\lceil 2.0 \rceil = 2$.

$|x|$ Indicates the absolute value of x: $|-17| = 17$, $|17| = 17$.

$\oplus$ Indicates exclusive OR (modulo-2 addition).

min (x, y) Indicates the minimum of x and y.

max (x, y) Indicates the maximum of x and y.

x mod y Indicates the remainder after dividing x by y: $x \bmod y = x - (y \times \lfloor x/y \rfloor)$.

Unless otherwise specified, the format of field values is unsigned binary.

Unless indicated otherwise, this standard presents numbers in decimal form. Binary numbers are distinguished in the text by the use of single quotation marks. Hexadecimal numbers are distinguished by the prefix '0x'.

Unless specified otherwise, each field of a packet shall be transmitted in sequence such that the most significant bit (MSB) is transmitted first and the least significant bit (LSB) is transmitted last. The MSB is the left-most bit in the figures in this document. If there are multiple rows in a table, the top-most row is transmitted first. Within a row in a table, the left-most bit is transmitted first.Notations of the form "repetition factor of N" or "repeated N times" mean that a total of N versions of the item are used.

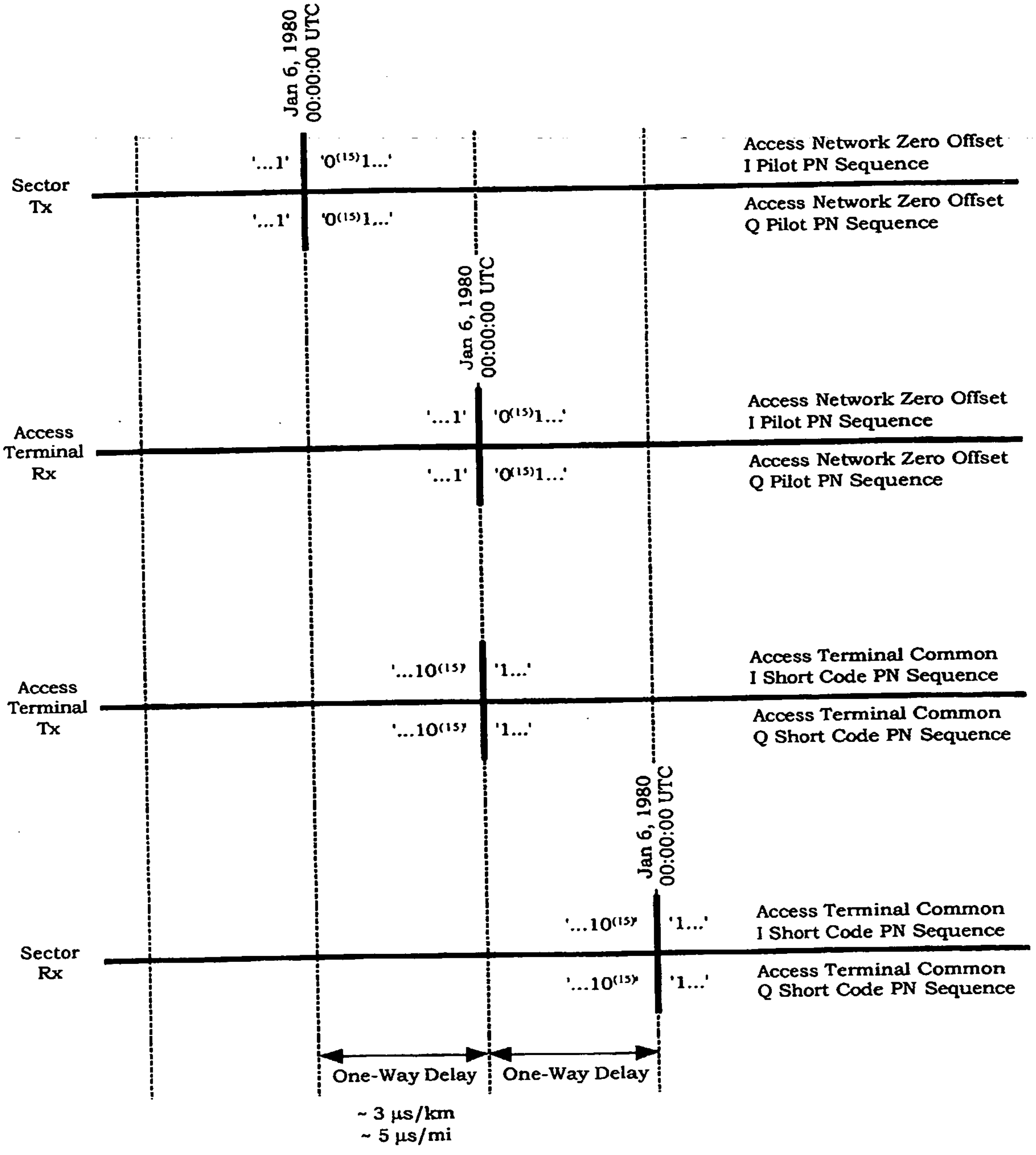
1.13 CDMA System Time

All sector air interface transmissions are referenced to a common system-wide timing reference that uses the Global Positioning System (GPS) time, which is traceable to and synchronous with Universal Coordinated Time (UTC). GPS and UTC differ by an integer number of seconds, specifically the number of leap second corrections added to UTC since January 6, 1980. The start of CDMA System Time is January 6, 1980 00:00:00 UTC, which coincides with the start of GPS time.

CDMA System Time keeps track of leap second corrections to UTC but does not use these corrections for physical adjustments to the CDMA System Time clocks.

Figure 1.13-1 shows the relation of CDMA System Time at various points in the system. The access network zero offset pilot PN sequences (as defined in 9.3.1.3.4) and the access terminal common short code PN sequences (as defined in 9.2.1.3.8.1) for the I and Q channels are shown in their initial states at the start of CDMA System Time. The initial state of the access network zero offset pilot PN sequences, both I and Q, is that state in which the next 15 outputs of the pilot PN sequence generator are '0'. The initial state of the access terminal common short code PN sequences, both I and Q, is that state in which the output of the short code PN sequence generator is the '1' following 15 consecutive '0' outputs.

From Figure 1.13-1, note that the CDMA System Time at various points in the transmission and the reception processes is the absolute time referenced at the access network antenna offset by the one-way or round-trip delay of the transmission, as appropriate. Time measurements are referenced to the transmit and receive antennas of the access network and the RF connector of the Access Terminal. The precise zero instant of CDMA System Time is the midpoint between the '1' prior to the 15 consecutive '0' outputs and the immediate succeeding '0' of the access network zero offset pilot PN sequences.



Notes:

(1) Time measurements are made at the antennas of Sectors and the RF connectors of the Access Terminals.

(2) $0^{(n)}$ denotes a sequence of n consecutive zeroes.

Figure 1.13-1. CDMA System Time Line

1.14 Revision Number

Access terminals and access networks complying with the requirements of this specification shall set their revision number to 0x01.

No text.

2 DEFAULT SIGNALING APPLICATION

2.1 Introduction

2.1.1 General Overview

The Default Signaling Application encompasses the Signaling Network Protocol (SNP) and the Signaling Link Protocol (SLP). Protocols in each layer use SNP to exchange messages. SNP is also used by application specific control messages.

SNP provides a single octet header that defines the Type of the protocol with which the message is associated. SNP uses the Type field to route the message to the appropriate protocol.

SLP provides message fragmentation, reliable and best-effort message delivery and duplicate detection for messages that are delivered reliably.

The relationship between SNP and SLP is illustrated in Figure 2.1.1-1.

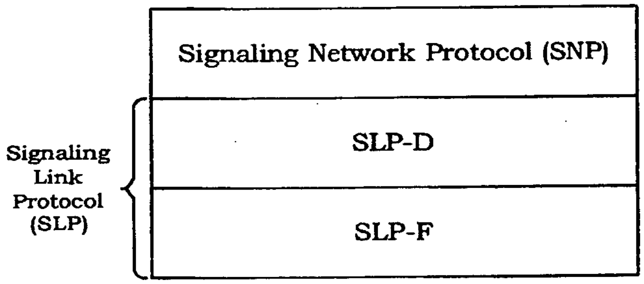

Signaling Network Protocol (SNP)
Signaling Link Protocol (SLP)
SLP-D
SLP-F

Figure 2.1.1-1. Default Signaling Layer Protocols

The Signaling Link Protocol consists of two sub-layers, the delivery layer, SLP-D, and the fragmentation layer, SLP-F.

2.1.2 Data Encapsulation

Figure 2.1.2-1 and Figure 2.1.2-2 illustrate the relationship between a message, SNP packets, SLP packets, and Stream Layer payloads. Figure 2.1.2-1 shows a case where SLP does not fragment the SNP packet. Figure 2.1.2-2 shows a case where the SLP fragments the SNP packet into more than one SLP-F payload.

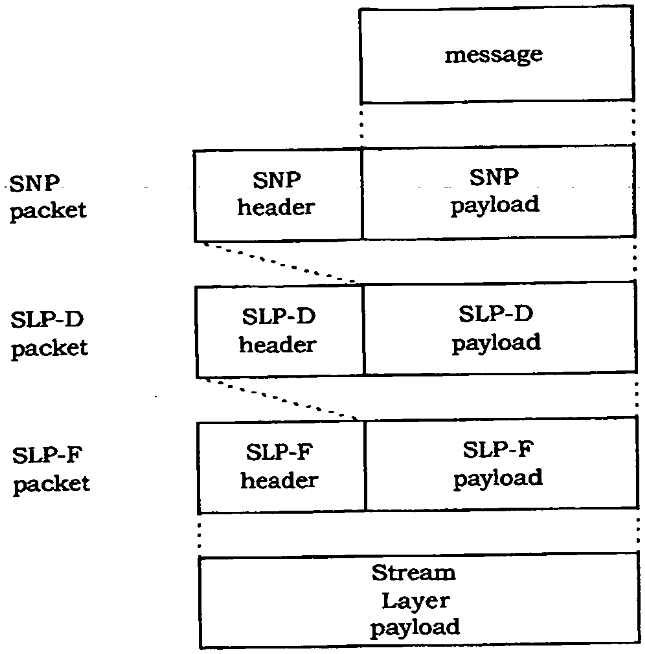


Figure 2.1.2-1. Message Encapsulation (Non-fragmented)

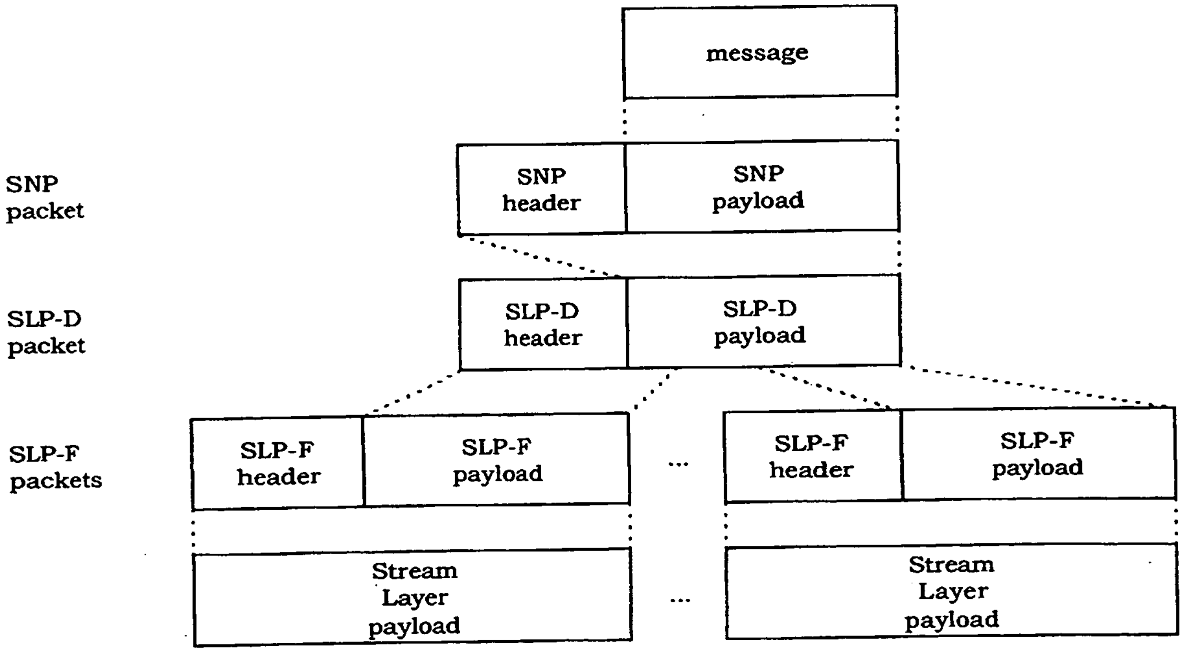


Figure 2.1.2-2. Message Encapsulation (Fragmented)

2.2 General Signaling Requirements

2.2.1 General Requirements

The following requirements are common to all protocols that carry messages using SNP and that provide for message extensibility. The access terminal and the access network shall abide by the following rules when generating and processing any signaling message carried by SNP.

- Messages are always an integer number of octets in length; and, if necessary, include a Reserved field at the end of the message to make them so. The receiver shall ignore the value of the Reserved fields.
- The first field of the message shall be transmitted first. Within each field, the most significant bit of the field shall be transmitted first.
- Message identifiers shall be unambiguous for each protocol Type and for each Subtype for all protocols compatible with the Air Interface, defined by MinimumRevision and above.
- For future revisions, the transmitter shall add new fields only at the end of a message (excluding any trailing Reserved field). The transmitter shall not add fields if their addition makes the parsing of previous fields ambiguous for receivers whose protocol revision is equal to or greater than MinimumRevision.
- The receiver shall discard all unrecognized messages.
- The receiver shall discard all unrecognized fields.
- The receiver shall discard a message if any of the fields in the message is set to a value outside of the defined field range, unless the receiver is specifically directed to ignore this field. A field value is outside of the allowed range if a range was specified with the field and the value is not in this range, or the field is set to a value that is defined as invalid. The receiver shall discard a field in a message if the field is set to a reserved value.

2.2.2 Message Information

Each message definition contains information regarding channels on which the message can be transmitted, whether the message requires SLP reliable or best-effort delivery, the addressing modes applicable to the message, and the message priority. This information is provided in the form of a table, an example of which is given in Figure 2.2.2-1.

Channels	CCsyn
Addressing	broadcast

SLP	Best Effort
Priority	30

Figure 2.2.2-1. Sample Message Information

The following values are defined:

- Channels: The Physical Layer channel on which this message can be transmitted. Values are:
  - CC for Control Channel (synchronous or asynchronous capsule),
  - CCsyn for Control Channel synchronous capsule,
  - AC for Access Channel,
  - FTC for Forward Traffic Channel, and
  - RTC for Reverse Traffic Channel.
- SLP: Signaling Link Protocol requirements. Values are:
  - Best Effort: the message is sent once and is subject to erasure, and
  - Reliable: erasures are detected and the message is retransmitted one or more times, if necessary.
- Addressing: Addressing modes for the message. Values are:
  - Broadcast if a broadcast address can be used with this message,
  - Multicast if a multicast address can be used with this message, and
  - Unicast if a unicast address can be used with this message.
- Priority: A number between 0 and 255 where lower numbers indicate higher priorities. The priority is used by the Connection Layer (specifically, the Packet Consolidation Protocol) in prioritizing the messages for transmission.

2.3 Signaling Network Protocol

2.3.1 Overview

The Signaling Network Protocol (SNP) is a message-routing protocol, and routes messages to protocols according to the Type field provided in the SNP header.

The actual protocol indicated by the Type is negotiated during session set-up. For example, Type 0x01 is associated with the Control Channel MAC Protocol. The specific Control Channel MAC Protocol used (and, therefore, the Control Channel MAC protocol generating and processing the messages delivered by SNP) is negotiated when the session is setup.

The remainder of the message following the Type field (SNP header) is processed by the protocol specified by the Type.

2.3.2 Primitives and Public Data

2.3.2.1 Commands

This protocol does not define any commands.

2.3.2.2 Return Indications

This protocol does not return any indications.

2.3.2.3 Public Data

The protocol shall make the Type value associated with protocols public.

2.3.3 Basic Protocol Numbers

SNP is a protocol associated with the Default Signaling Application. The application subtype for this application is defined in Table 4.2.6.2.1.1-1.

2.3.4 Protocol Data Unit

The protocol data unit for this protocol is an SNP packet. Each SNP packet consists of one message sent by a protocol using SNP.

The protocol constructs an SNP packet by adding the SNP header (see 2.3.7) in front of the payload. The structure of the SNP packet is shown in Figure 2.3.4-1.

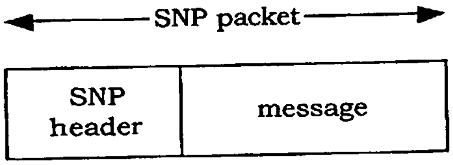


Figure 2.3.4-1. SNP Packet Structure

2.3.5 Procedures

SNP receives messages for transmission from multiple protocols. SNP shall add the Type field to each message and forward it for transmission to SLP.

SNP receives messages from SLP. SNP shall route these messages to their associated protocols according to the value of the Type field in the SNP header.

If an SNP message is to be transmitted on the Forward Traffic Channel or on the Reverse Traffic Channel, and if a connection is not open, SNP shall issue an ***AirLinkManagementProtocol.OpenConnection*** command. SNP should queue all messages requiring transmission in the Forward Traffic Channel or in the Reverse Traffic Channel until the protocol receives an ***IdleState.ConnectionOpened*** indication.

When SNP receives an ***SLP.Reset*** indication, it shall refrain from passing messages from protocols other than SLP for transmission to SLP until it receives an ***SLP.ResetAcked*** indication.

2.3.6 Type Definitions

Type definitions associated with the default protocol stack are presented in Table 2.3.6-1. The constant name and protocol layer are provided for informational purposes.

Table 2.3.6-1. Default Protocol Stack Type Values

Type	Protocol	Constant Name	Layer
0x14	Stream 0 Application	$N_{APP0Type}$	Application
0x15	Stream 1 Application	$N_{APP1Type}$	Application
0x16	Stream 2 Application	$N_{APP2Type}$	Application
0x17	Stream 3 Application	$N_{APP3Type}$	Application
0x13	Stream Protocol	$N_{STRType}$	Stream
0x10	Session Management Protocol	$N_{SMPType}$	Session
0x11	Address Management Protocol	$N_{ADMPType}$	Session
0x12	Session Configuration Protocol	$N_{SCPType}$	Session
0x0a	Air Link Management Protocol	$N_{ALMPType}$	Connection
0x0b	Initialization State Protocol	$N_{ISPType}$	Connection
0x0c	Idle State Protocol	$N_{IDPType}$	Connection
0x0d	Connected State Protocol	$N_{CSPType}$	Connection
0x0e	Route Update Protocol	$N_{RUPType}$	Connection
0x0f	Overhead Messages Protocol	$N_{OMPType}$	Connection
0x09	Packet Consolidation Protocol	$N_{PCPType}$	Connection
0x08	Security Protocol	N_{SPType}	Security
0x05	Key Exchange Protocol	$N_{KEPType}$	Security
0x06	Authentication Protocol	N_{APType}	Security
0x07	Encryption Protocol	N_{EPType}	Security
0x01	Control Channel MAC Protocol	$N_{CCMPType}$	MAC
0x02	Access Channel MAC Protocol	$N_{ACMPType}$	MAC
0x03	Forward Traffic Channel MAC Protocol	$N_{FTCMPType}$	MAC
0x04	Reverse Traffic Channel MAC Protocol	$N_{RTCMPType}$	MAC
0x00	Physical Layer Protocol	$N_{PHYType}$	Physical

2.3.7 SNP Header

The SNP shall place the following header in front of every message that it sends:

Field	Length (bits)
Type	8

Type Protocol Type. This field shall be set the Type value for the protocol associated with the encapsulated message.

2.3.8 Interface to Other Protocols

2.3.8.1 Commands

This protocol issues the following command:

AirLinkManagementProtocol.OpenConnection

2.3.8.2 Indications

This protocol registers to receive the following indications:

- ***IdleState.ConnectionOpened***
- ***SLP.Reset***
- ***SLP.ResetAcked***

2.4 Signaling Link Protocol

2.4.1 Overview

The Signaling Link Protocol (SLP) has two layers: The delivery layer and the fragmentation layer.

The purpose of the SLP delivery layer (SLP-D) is to provide best effort and reliable delivery for SNP packets. SLP-D provides duplicate detection and retransmission for messages using reliable delivery. SLP-D does not ensure in-order delivery of SNP packets.

The purpose of the SLP fragmentation layer (SLP-F) is to provide fragmentation for SLP-D packets.

2.4.2 Primitives and Public Data

2.4.2.1 Commands

This protocol does not define any commands.

2.4.2.2 Return Indications

This protocol returns the following indications:

- ***Reset***
- ***ResetAcked***

2.4.2.3 Public Data

- None.

2.4.3 Basic Protocol Numbers

SLP is a protocol associated with the default signaling application. The application subtype for this application is defined in Table 4.2.6.2.1.1-1.

2.4.4 Protocol Data Unit

The protocol data units of this protocol are an SLP-D packet and an SLP-F packet.

2.4.5 Procedures

Unless explicitly specified, SLP requirements for the access terminal and the access network are identical; and are, therefore, presented in terms of sender and receiver.

2.4.5.1 Reset

SLP can only be reset at the initiative of the access network. To reset SLP, the access network shall perform the following:

- The access network shall initialize its data structures as described in 2.4.5.3.2 and 2.4.5.2.3.2,

- The access network shall return a ***Reset*** indication, and
- The access network shall send a Reset message.

Upon receiving a Reset message, the access terminal shall validate the message sequence number as defined in 10.6. If the message is valid, the access terminal shall respond with a ResetAck message and shall initialize its data structures as described in 2.4.5.3.2 and 2.4.5.2.3.2. If the message sequence number of the Reset message is not valid, the access terminal shall discard the message.

The SLP protocol in the access network shall return a ***ResetAcked*** indication when it receives a ResetAck message with a MessageSequence field equal to the MessageSequence sent in the Reset message. The access network shall increment the sequence number for every Reset message it sends.

The access terminal shall initialize the reset receive pointer used to validate Reset messages (see 10.6) to 0 when the protocol receives a ***SessionManagement.BootCompleted*** indication.

2.4.5.2 Delivery Layer Procedures

2.4.5.2.1 General Procedures

These procedures apply to both the best effort and reliable delivery.

2.4.5.2.1.1 Transmitter Requirements

The transmitter shall take the packet from the upper layer and add the SLP-D header.

The transmitter shall forward the resulting SLP-D packet to the SLP fragmentation layer.

2.4.5.2.1.2 Receiver Requirements

The receiver shall forward the AckSequenceNumber field of the SLP-D header to the co-located transmitter (see 2.4.5.2.3.3.1).

2.4.5.2.2 Best Effort Delivery Procedures

2.4.5.2.2.1 Transmitter Requirements

The transmitter shall set the SequenceValid field of a best-effort SLP-D packet to '0'.

2.4.5.2.2.2 Receiver Requirements

The receiver shall forward the SLP-D payload to the upper layer.

2.4.5.2.3 Reliable Delivery Procedures

2.4.5.2.3.1 Overview

SLP-D is an Ack-based protocol with a sequence space of ***S*** = 3 bits.

SLP-D maintains the following variables for reliable delivery SLP-D packet payloads:

- *V(S)* The sequence number of the next SLP-D packet to be sent.
- *V(N)* The sequence number of the next expected SLP-D packet.
- Rx A 2^S bit vector. Rx[*i*] = '1' if the SLP-D packet with sequence number *i* was received.

2.4.5.2.3.2 Initialization

When SLP-D is initialized or reset it shall perform the following:

- Set the send state variable ***V(S)*** to zero in the transmitter.
- Set the receive state variable ***V(N)*** to zero in the receiver.
- Set Rx[i] to '0' for i = 0...2^S-1.
- Clear the retransmission and resequencing buffers.
- Discard any SLP-D packets queued for retransmission.

When SLP-D is initialized or is reset, the sender shall begin sending SLP-D packets with an initial SequenceNumber of 0.

The access terminal and the access network shall perform the initialization procedure if the protocol receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication.

2.4.5.2.3.3 Data Transfer

All operations and comparisons performed on SLP-D packet sequence numbers shall be carried out in unsigned modulo 2^S arithmetic. For any SLP-D packet sequence number ***N***, the sequence numbers in the range [$N+1, N+2^{S-1}-1$] shall be considered greater than ***N*** and the numbers in the range [$N-2^{S-1}, N-1$] shall be considered smaller than ***N***.

2.4.5.2.3.3.1 Transmit Procedures

The transmitter shall set the SequenceValid field of a reliable-delivery SLP-D packet to '1'.

The transmitter shall acknowledge each reliable-delivery SLP-D packet that its co-located receiver received. The transmitter shall send an acknowledgment within $T_{SLPSDUAck}$ seconds of the receiver receiving a reliable-delivery SLP-D packet. The transmitter acknowledges the received SLP-D packet by setting the AckSequenceNumber field of a transmitted SLP-D packet to the SequenceNumber field of the SLP-D packet being acknowledged, and by setting the AckSequenceValid field to '1'. The transmitter may use the AckSequenceNumber field of an SLP-D it is transmitting; or, if none is available within the required acknowledgment time, it shall transmit an SLP-D header-only SLP-D packet carrying the acknowledgment. The SLP-D header-only SLP-D packet shall be sent as a best-effort SLP-D packet.

Acknowledging an SLP-D packet with sequence number ***N*** does not imply an acknowledgement for an SLP-D packet with a sequence number smaller than ***N***.

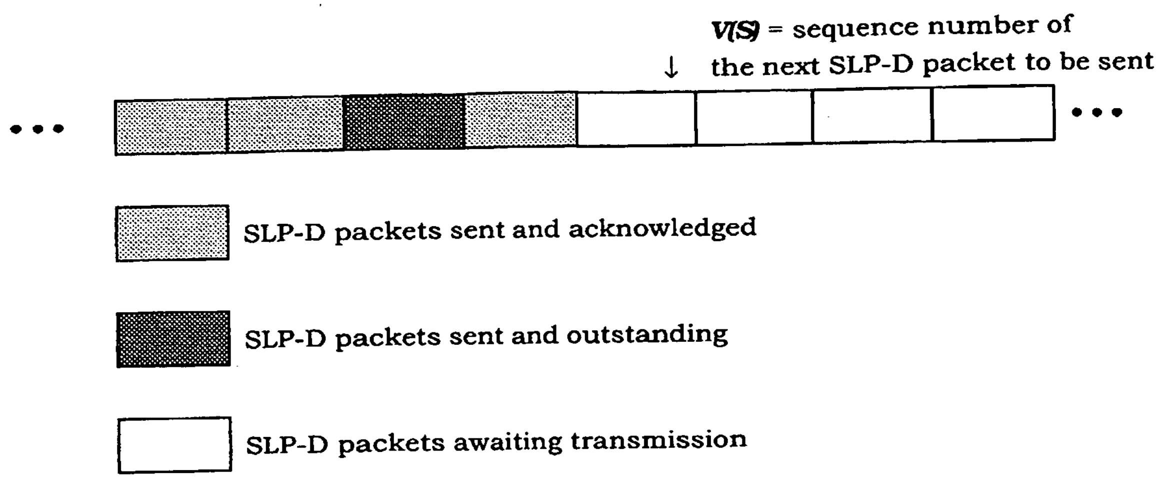

V(S) = sequence number of
the next SLP-D packet to be sent
• • •
• • •
SLP-D packets sent and acknowledged
SLP-D packets sent and outstanding
SLP-D packets awaiting transmission

Figure 2.4.5.2.3.3.1-1. SLP-D Transmit Sequence Number Variable

The transmitter shall maintain an ***S***-bit variable ***V(S)***. The sequence number field (SequenceNumber) in each new SLP-D packet transmitted shall be set to ***V(S)***. After transmitting the SLP-D packet, ***V(S)*** shall be incremented.

If SLP-D has already transmitted 2^{S-1} SLP-D packets, SLP-D shall transmit an SDU with sequence number ***n***, only after receiving acknowledgments for the SLP-D packets transmitted with sequence number ***n*** - 2^{S-1} and below, or after determining that these SLP-D packets could not be delivered.

If the transmitter does not receive from its co-located receiver an AckSequenceNumber equal to the SequenceNumber of an outstanding SLP-D packet within $T_{SLPWaitAck}$ seconds, the transmitter shall retransmit the SLP-D packet. The transmitter shall attempt to transmit an SLP-D packet for a maximum of $N_{SLPAttempt}$.

The transmitter shall provide a retransmission buffer for 2^{S-1} SLP-D packets. Reliable-delivery SLP-D packets shall be stored in the buffer when they are first transmitted and may be deleted from the buffer, when they are acknowledged or when SLP-D determines that they could not be delivered.

2.4.5.2.3.3.2 Receive Procedures

The SLP-D reliable-delivery receiver shall maintain an ***S***-bit variable ***V(N)***. ***V(N)*** contains the sequence number of the next expected SLP-D packet.

The receiver shall maintain a vector Rx with 2^{S} one-bit elements. Rx[***k***] is set to '1' if the SLP-D packet with sequence number ***k*** has been received.

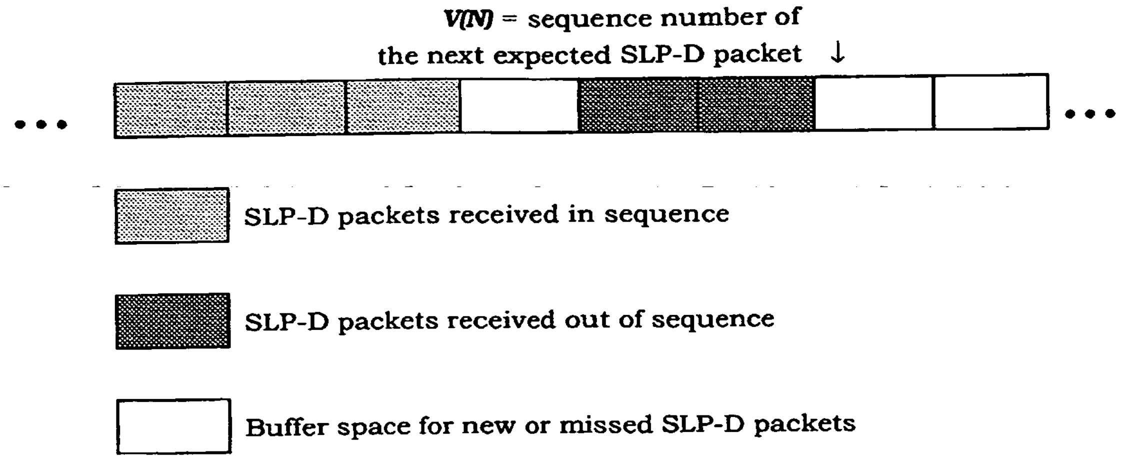

V(N) = sequence number of
the next expected SLP-D packet
SLP-D packets received in sequence
SLP-D packets received out of sequence
Buffer space for new or missed SLP-D packets

Figure 2.4.5.2.3.3.2-1. SLP Receive Sequence Number Variables

For each received SLP-D packet, the receiver shall perform the following actions:

- If a received SLP-D packet has a sequence number k that is smaller than ***V(N)*** and Rx[***k***] = '1', SLP-D shall discard it as a duplicate.
- If a received SLP-D packet has a sequence number k that is smaller than ***V(N)*** and Rx[***k***] = '0', SLP-D shall set Rx[k] to '1' and pass the SLP-D payload to the upper layer.
- If a received SLP-D packet has sequence number k that is equal to ***V(N)***, SLP-D shall set Rx[***k***] to '1' and Rx[$k+2^{S-1}$] to '0'. SLP-D shall set ***V(N)*** to ***k+1*** and pass the SLP-D payload to the upper layer.
- If a received SLP-D packet has a sequence number k that is greater than ***V(N)***, SLP-D shall set Rx[***k***] to '1', and Rx[***v***] to '0' for all ***v > k***. SLP-D shall set ***V(N)*** to ***k+1*** and pass the SLP-D payload to the upper layer.

2.4.5.3 Fragmentation Layer Procedures

2.4.5.3.1 Overview

SLP-F is a self-synchronizing loss detection protocol with a sequence space of ***S*** = 6 bits.

SLP-F maintains the following variables for SLP-F packets:

- *V(S)* The sequence number of the next SLP-F packet to be sent.
- Sync The SLP-F synchronized status flag.

2.4.5.3.2 Initialization

When SLP-F is initialized or reset it shall perform the following:

- Set the send state variable ***V(S)*** to zero in the transmitter.
- Set Sync to zero.
- Clear the re-assembly buffers.

When SLP-F is initialized or reset, the sender shall begin sending SLP-F packets with an initial SequenceNumber of 0.

The access terminal and the access network shall perform the initialization procedure if the protocol receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication.

2.4.5.3.3 Data Transfer

All operations and comparisons performed on SLP-F packet sequence numbers shall be carried out in unsigned modulo 2^S arithmetic.

2.4.5.3.4 Sender Requirements

The sender shall construct the SLP-F packet(s) by adding the SLP-F header, defined in 2.4.6.1, in front of each SLP-F payload. The size of each SLP-F packet shall not exceed the current maximum SLP-F packet size.

The sender shall construct the SLP-F payload(s) from an SLP-D packet. If the SLP-D packet exceeds the current maximum SLP-F payload size, then the sender shall fragment the SLP-D packet. If the sender does not fragment the SLP-D packet, then the SLP-D packet is the SLP-F payload. If the sender does fragment the SLP-D packet, then each SLP-D packet fragment is an SLP-F payload.

If the SLP-F payload contains the beginning of an SLP-D packet, then the sender shall set the SLP-F header Begin field to '1'; otherwise, the sender shall set the SLP-F header Begin field to '0'.

If the SLP-F payload contains the end of an SLP-D packet, then the sender shall set the SLP-F header End field to '1'; otherwise, the sender shall set the SLP-F header End field to '0'

The sender shall set the SLP-F SequenceNumber field to ***V(S)***.

If the SLP-F payload contains a complete SLP-D packet, then the sender shall not include the SLP-F header Begin, End and SequenceNumber fields; otherwise, the sender shall include the SLP-F header Begin, End and SequenceNumber fields.

The sender shall increment the ***V(S)*** each time it sends a new SLP-F packet.

2.4.5.3.5 Receiver Requirements

The receiver shall maintain a re-assembly buffer to which it writes the SLP-F payloads when the Sync variable of the SLP-F protocol is equal to 1. The receiver shall perform the following in the order specified:

- If the SLP-F header Fragmented field is '0', then the receiver shall assume the SLP-F header Begin field is '1', the SLP-F header End field is '1' and the SLP-F header SequenceNumber is '0'.

- If the SequenceNumber of the current SLP-F packet is not one greater than SequenceNumber of the last SLP-F packet whose payload was written to the re-assembly buffer, then the receiver shall discard the contents of the re-assembly buffer and shall set the Sync flag to '0'.
- If the Begin field is '1', then the receiver shall discard the contents of the re-assembly buffer and set the Sync flag to '1'.
- If the Sync flag is '1', then the receiver shall write the SLP-F payload to the re-assembly buffer, otherwise the receiver shall discard the SLP-F payload.
- If the End field is '1', then the receiver shall pass the contents of the re-assembly buffer to the upper layer and set the Sync flag to '0'.

2.4.6 Header Formats

The combined SLP-D and SLP-F header length, x, is such that

x modulo 8 = 6.

2.4.6.1 SLP-F Header

The SLP-F header length, x, is such that

x modulo 8 = 5; if the SLP-F payload contains an SLP-D packet with SLP-D header,

x modulo 8 = 6; if the SLP-F payload contains an SLP-D packet without SLP-D header,

The SLP-F header has the following format:

Field	Length(bits)
Reserved	4
Fragmented	1
Begin	0 or 1
End	0 or 1
SequenceNumber	0 or 6
OctetAlignmentPad	0 or 1

Reserved The sender shall set this field to zero. The receiver shall ignore this field.

Fragmented SLP-F header fragmentation indicator. If the rest of the SLP-F header is included, then the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'. If the SLP-F payload contains a complete SLP-D packet, the sender shall not include the rest of the

SLP-F header; otherwise, the sender shall include the rest of the SLP-F header.

Begin — Start of SLP-D packet flag. The sender shall only include this field if the Fragmented field is set to '1'. If this SLP-F payload contains the beginning of an SLP-D packet, then the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'.

End — End of SLP-D packet flag. The sender shall only include this field if the Fragmented field is set to '1'. If this SLP-F payload contains the end of an SLP-D packet, the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'.

SequenceNumber — SLP-F packet sequence number. The sender shall only include this field if the Fragmented field is set to '1'. The sender shall increment this field for each new SLP-F packet sent.

OctetAlignmentPad — Octet alignment padding. The sender shall include this field and set it to '0' if the Fragmented field is set to '1' and Begin field is set to '0'. Otherwise, the sender shall omit this field.

2.4.6.2 SLP-D Header

The SLP-D header length, x, is such that

$$x \text{ modulo } 8 = 1.$$

The SLP-D header has the following format:

Field	Length(bits)
FullHeaderIncluded	1
AckSequenceValid	0 or 1
AckSequenceNumber	0 or 3
SequenceValid	0 or 1
SequenceNumber	0 or 3

FullHeaderIncluded — SLP-D header included flag. If the rest of SLP-D header is included, then the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'. If the sender is either sending or acknowledging a reliable-delivery SLP-D payload, then the sender shall include the rest of the SLP-D header; otherwise, the sender shall not include the rest of the SLP-D header.

AckSequenceValid — The sender shall only include this field if the FullHeaderIncluded field is set to '1'. If the AckSequenceNumber field contains a valid value, then the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'. If the sender is acknowledging a reliable-delivery SLP-D payload, then the sender shall include a valid AckSequenceNumber field; otherwise, the sender shall not include a valid AckSequenceNumber field.

AckSequenceNumber

The sender shall only include this field if the FullHeaderIncluded field is set to '1'. If the AckSequenceValid field is set to '1', then the sender shall set this field to the sequence number of the first reliable-delivery SLP-D payload that has not been acknowledged; otherwise, the sender shall set this field to zero. If the AckSequenceValid field is set to '0', then the receiver shall ignore this field.

SequenceValid The sender shall only include this field if the FullHeaderIncluded field is set to '1'. If the SequenceNumber field contains a valid value, then the sender shall set this field to '1'; otherwise, the sender shall set this field to '0'. If the sender is sending a reliable-delivery SLP-D payload, then the sender shall include a valid SequenceNumber field.

SequenceNumber The sender shall only include this field if the FullHeaderIncluded field is set to '1'. If the SequenceValid field is set to '1', then the sender shall set this field to the sequence number of the reliable SLP-D payload; otherwise, the sender shall set this field to zero. If the SequenceValid field is set to '0', then the receiver shall ignore this field.

2.4.7 Message Formats

2.4.7.1 Reset

The Reset message is used by the access network to reset SLP.

Field	Length (bits)
MessageID	8
MessageSequence	8

MessageID The access network shall set this field to 0x00.

MessageSequence The access network shall increment this field for every new Reset message it sends.

Channels	CC FTC
Addressing	unicast

SLP	Best Effort
Priority	40

2.4.7.2 ResetAck

The ResetAck message is used by the access terminal to complete an SLP reset.

Field	Length (bits)
MessageID	8
MessageSequence	8

MessageID The access terminal shall set this field to 0x01.

MessageSequence The access terminal shall set this field to the sequence number of the associated Reset message.

Channels	RTC
Addressing	unicast

SLP	Best Effort
Priority	40

2.4.8 Protocol Numeric Constants

Constant	Meaning	Value
$T_{SLPSDUAck}$	Time for receiver to acknowledge an arriving reliable-delivery SDU	200 ms
$N_{SLPAttempt}$	Number of times to retry sending a reliable-delivery SDU	3
$T_{SLPWaitAck}$	Retransmission timer for a reliable-delivery SDU	400 ms

2.4.9 Interface to Other Protocols

2.4.9.1 Commands

This protocol does not issue any commands.

2.4.9.2 Indications

This protocol registers to receive the following indications:

- *ReverseTrafficChannelMAC.LinkAcquired*
- *SessionManagement.BootCompleted*

No text.

3 DEFAULT PACKET APPLICATION

3.1 Introduction

3.1.1 General Overview

The Default Packet Application provides an octet stream that can be used to carry packets between the access terminal and the access network.

The Default Packet Application provides:

- The functionality defined in [1].
- The Radio Link Protocol (RLP), which provides in-order delivery of RLP packets, retransmission, and duplicate detection, thus, reducing the radio link error rate as seen by the higher layer protocols.
- Packet Location Update Protocol, which defines location update procedures and messages in support of mobility management for the Packet Application.
- Flow Control Protocol, which provides flow control for the Default Packet Application Protocol.

The relationship between the Default Packet Application protocols is illustrated in Figure 3.1.1-1.

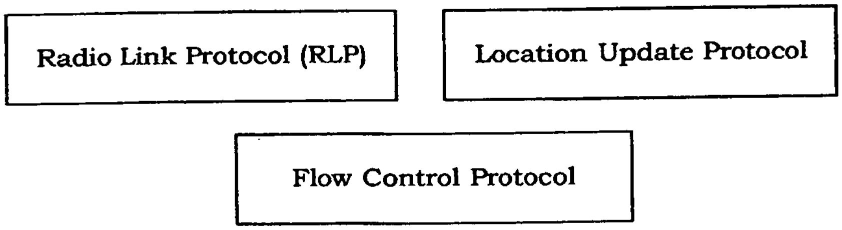


Figure 3.1.1-1. Default Packet Application Protocols

3.1.2 Data Encapsulation

Figure 3.1.2-1 illustrates the relationship between the octet stream from the upper layer, an RLP packet, and a Stream Layer payload.

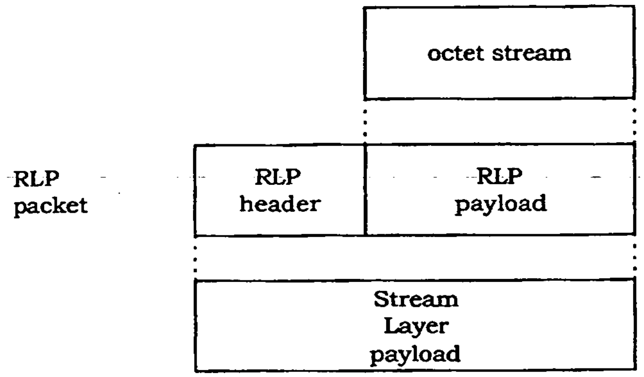


Figure 3.1.2-1. Default Packet Application Encapsulation

3.2 Radio Link Protocol

3.2.1 Overview

The Radio Link Protocol (RLP) provides an octet stream service with an acceptably low erasure rate for efficient operation of higher layer protocols (e.g., TCP). When used as part of the Default Packet Application, the protocol carries an octet stream from the upper layer.

RLP uses Nak-based retransmissions. If the receiver fails to receive octets whose retransmission it requested once, the receiver forwards whatever octets it has to the upper layer and continues reception beyond the missing octets.

3.2.2 Primitives and Public Data

3.2.2.1 Commands

This protocol does not define any commands.

3.2.2.2 Return Indications

This protocol does not return any indications.

3.2.2.3 Public Data

- None.

3.2.3 Basic Protocol Numbers

RLP is a protocol associated with the default packet application. The application identifier for this application is defined in Table 4.2.6.2.1.1-1.

3.2.4 Protocol Data Unit

The transmission unit of this protocol is an RLP packet.

RLP is unaware of higher layer framing; it operates on a featureless octet stream, delivering the octets in the order received from the higher layer.

RLP receives octets for transmission from the higher layer and forms an RLP packet by concatenating the RLP packet header defined in 3.2.6.1 with a number of received contiguous octets. The policy RLP follows in determining the number of octets to send in an RLP packet is beyond the scope of this specification. It is subject to the requirement that an RLP packet shall not exceed the maximum payload length that can be carried by a Stream Layer packet given the target channel and current transmission rate on that channel.

RLP makes use of the Reset, ResetAck, and Nak messages to perform control related operations. When RLP sends these messages it shall use the Signaling Application.

3.2.5 Procedures

3.2.5.1 Initialization and Reset

The RLP initialization procedure initializes the RLP variables and data structures in one end of the link. The RLP reset procedure guarantees that RLP state variables on both sides are synchronized. The reset procedure includes initialization.

The access terminal and the access network shall perform the Initialization Procedure defined in 3.2.5.1.1 if the protocol receives an ***IdleState.ConnectionOpened*** indication.

3.2.5.1.1 Initialization Procedure

When RLP performs the initialization procedure it shall:

- Reset the send state variable ***V(S)*** to zero,
- reset the receive state variables ***V(R)*** and ***V(N)*** to zero,
- clear the resequencing buffer, and
- clear the retransmission queues.

3.2.5.1.2 Reset Procedure

3.2.5.1.2.1 Reset Procedure for the Initiating Side

The side initiating a reset procedure sends a Reset message and enters the RLP Reset State.

Upon entering the RLP Reset state RLP shall:

- Perform the initialization procedure defined in 3.2.5.1.1.
- Ignore all RLP data octets received while in the RLP Reset state.
- If RLP receives a ResetAck message while in the RLP Reset state, it shall send a ResetAck message back and leave the RLP Reset state.

If a ResetAck message is received while RLP is not in the RLP Reset state, the message shall be ignored.

3.2.5.1.2.2 Reset Procedure for the Responding Side

When RLP receives a Reset message, it shall respond with a ResetAck message. After sending the message it shall enter the RLP Reset state, if it was not already in the RLP reset state. Upon entering the RLP Reset state RLP shall:

- Perform the initialization procedure defined in 3.2.5.1.1.
- Ignore all RLP data octets received while in the RLP Reset state.
- When RLP receives a ResetAck message, it shall leave the RLP reset state.

If a ResetAck is received while RLP is not in the RLP Reset state, the message shall be ignored.

3.2.5.2 Data Transfer

RLP is a Nak-based protocol with a sequence space of ***S*** bits, where $\boldsymbol{S} = 22$.

All operations and comparisons performed on RLP packet sequence numbers shall be carried out in unsigned modulo 2^S arithmetic. For any RLP octet sequence number ***N***, the sequence numbers in the range $[\boldsymbol{N+1}, \boldsymbol{N}+2^{S-1}\boldsymbol{-1}]$ shall be considered greater than ***N*** and the sequence numbers in the range $[\boldsymbol{N-2^{S-1}}, \boldsymbol{N-1}]$ shall be considered smaller than ***N***.

3.2.5.2.1 RLP Transmit Procedures

The RLP transmitter shall maintain an ***S***-bit variable ***V(S)*** for all transmitted RLP data octets (see Figure 3.2.5.2.1-1). ***V(S)*** is the sequence number of the next RLP data octet to be sent. The sequence number field (SEQ) in each new RLP packet transmitted shall be set to ***V(S)***, corresponding to the sequence number of the first octet in the packet. The sequence number of the i^{th} octet in the packet (with the first octet being octet 0) is implicitly given by SEQ+*i*. ***V(S)*** shall be incremented for each octet contained in the packet.

After transmitting a packet, the RLP transmitter shall start an RLP flush timer for time $T_{RLPFlush}$. If the RLP transmitter sends another packet before the RLP flush timer expires, the RLP transmitter shall reset and restart the timer. If the timer expires, the RLP transmitter shall disable the flush timer and the RLP transmitter shall send an RLP packet containing the octet with sequence number ***V(S)***-1. The RLP transmitter should allow sufficient time before deleting a packet transmitted for the first time.

Upon receiving a Nak message, RLP shall insert a copy of the requested octet(s) into its output stream if those octets are available. If the Nak record includes any sequence number greater than or equal to ***V(S)***, RLP shall perform the reset procedures specified in 3.2.5.1.2. If the Nak record does not include any sequence number greater than or equal to ***V(S)*** but the requested octets are not available for retransmissions, RLP shall ignore the Nak.

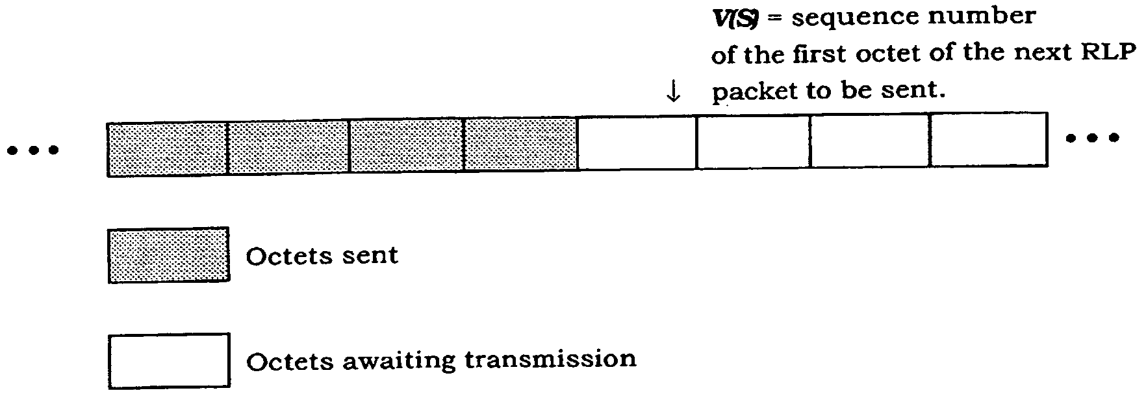

V(S) = sequence number of the first octet of the next RLP packet to be sent.
Octets sent
Octets awaiting transmission

Figure 3.2.5.2.1-1. RLP Transmit Sequence Number Variable

RLP shall assign the following priorities to RLP packets:

- Packet containing re-transmitted octets: 60
- Packet containing octets transmitted for the first time: 70

3.2.5.2.2 RLP Receive Procedures

The RLP receiver shall maintain two S-bit variables for receiving, ***V(R)*** and ***V(N)*** (see Figure 3.2.5.2.2-1). ***V(R)*** contains the sequence number of the next octet expected to arrive. ***V(N)*** contains the sequence number of the first missing octet, as described below.

In addition, the RLP receiver shall keep track of the status of each octet in its resequencing buffer indicating whether the octet was received or not. Use of this status is implied in the following procedures.

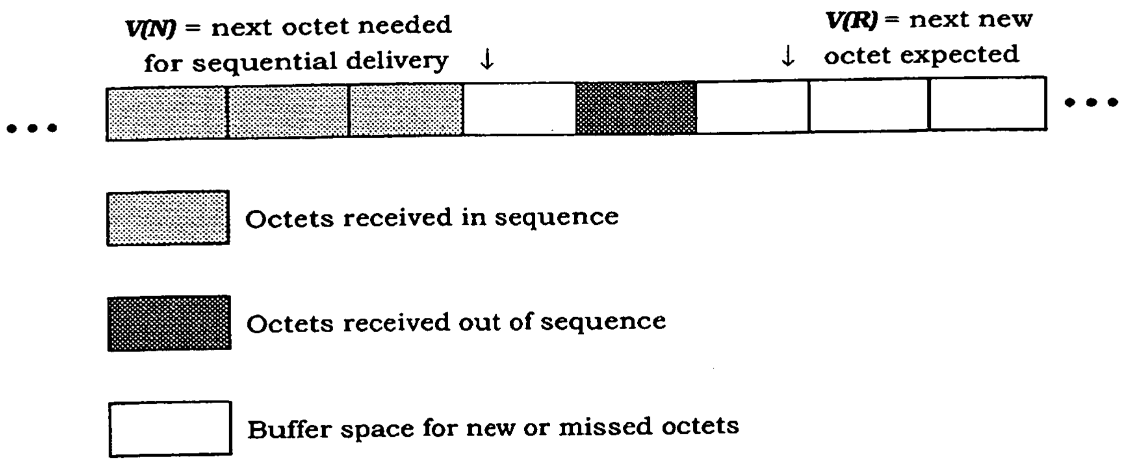

V(N) = next octet needed for sequential delivery
V(R) = next new octet expected
Octets received in sequence
Octets received out of sequence
Buffer space for new or missed octets

Figure 3.2.5.2.2-1. RLP Receive Sequence Number Variables

In the following, **X** denotes the sequence number of a received octet. For each received octet, RLP shall perform the following procedures:

- If ***X*** < ***V(N)***, the octet shall be discarded as a duplicate.
- If ***V(N)*** ≤ ***X*** < ***V(R)***, and the octet is not already stored in the resequencing buffer, then:
  - RLP shall store the received octet in the resequencing buffer.
  - If ***X*** = ***V(N)***, RLP shall pass all contiguous octets in the resequencing buffer, from ***V(N)*** upward, to the higher layer, and may remove the passed octets from the resequencing buffer. RLP shall then set ***V(N)*** to (LAST+1) where LAST is the sequence number of the last octet passed to the higher layer from the resequencing buffer.
- If ***V(N)*** < ***X*** < ***V(R)***, and the octet has already been stored in the resequencing buffer, then the octet shall be discarded as a duplicate.
- If X = ***V(R)***, then:
  - If ***V(R)*** = ***V(N)***, RLP shall increment ***V(N)*** and ***V(R)*** and shall pass the octet to the higher layer.
  - If ***V(R)*** ≠ ***V(N)***, RLP shall increment ***V(R)*** and shall store the octet in the resequencing buffer.
- If ***X*** > ***V(R)***, then:
  - RLP shall store the octet in the resequencing buffer.
  - RLP shall send a Nak message requesting the retransmission of all missing RLP octets from ***V(R)*** to ***X***-1, inclusive.
  - RLP shall set ***V(R)*** to ***X***+1.

RLP shall set a Nak abort timer for each data octet requested in a Nak record for a period of $T_{RLPAbort}$. If a requested octet has not arrived when its Nak abort timer expires, RLP shall pass all octets in the resequencing buffer up to the missing octet, in order of sequence number, to the higher layer. RLP shall skip any missing octets. RLP shall set ***V(N)*** to the sequence number of the next missing octet, or to ***V(R)*** if there are no remaining missing octets. Further recovery is the responsibility of the upper layer protocols.

3.2.6 RLP Packet Header

3.2.6.1 RLP Packet Header

The RLP packet header, which precedes the RLP payload, has the following format:

Field	Length (bits)
SEQ	22

SEQ The RLP sequence number of the first octet in the RLP payload.

3.2.7 Message Formats

The messages described in this section control the function of the RLP. These messages are exchanged between the access terminal and the access network using the SNP.

3.2.7.1 Reset

The access terminal and the access network send the Reset message to reset RLP.

Field	Length (bits)
MessageID	8

MessageID The sender shall set this field to 0x00.

Channels	CC FTC RTC
Addressing	unicast

SLP	Reliable
Priority	50

3.2.7.2 ResetAck

The access terminal and the access network send the ResetAck message to complete the RLP reset procedure.

Field	Length (bits)
MessageID	8

MessageID The sender shall set this field to 0x01.

Channels	CC FTC RTC
Addressing	unicast

SLP	Reliable
Priority	50

3.2.7.3 Nak

The access terminal and the access network send the Nak message to request the retransmission of one or more octets.

Field	Length (bits)
MessageID	8
NakRequests	8
NakRequests occurrences of the following three fields:	
Reserved	2
FirstErased	22
WindowLen	16

MessageID The sender shall set this field to 0x02.

NakRequests The sender shall set this field to the number of Nak requests included in this message. The sender shall include NakRequests occurrences of the following three fields with the message.

Reserved The sender shall set this field to zero. The receiver shall ignore this field.

FirstErased The sender shall set this field to the sequence number of the first RLP octet erased in a sequence of erased octets whose retransmission is requested.

WindowLen The sender shall set this field to the length of the erased window. The receiver shall retransmit all the octets in the range FirstErased to FirstErased+WindowLen-1, inclusive.

Channels	CC	FTC	RTC	SLP	Best Effort
Addressing			unicast	Priority	50

3.2.8 Protocol Numeric Constants

Constant	Meaning	Value
$T_{RLPAbort}$	Time to wait for a retransmission of an octet requested in a Nak message	500 ms
$T_{RLPFlush}$	Time to wait before retransmitting the last transmitted octet	300 ms

3.2.9 Interface to Other Protocols

3.2.9.1 Commands

This protocol does not issue any commands.

3.2.9.2 Indications

This protocol registers to receive the following indications:

- ***IdleState.ConnectionOpened***

3.3 Location Update Protocol

3.3.1 Overview

The Location Update Protocol

- Defines location update procedures and messages for mobility management for the Default Packet Application, and
- Negotiates a PDSN selection method and provide data required for PDSN selection.

3.3.2 Primitives and Public Data

3.3.2.1 Commands

This protocol does not define any commands.

3.3.2.2 Return Indications

This protocol does not return any indications.

3.3.2.3 Public Data

- None.

3.3.3 Basic Protocol Numbers

Packet Location Update Protocol is a protocol associated with the Default Packet Application. The application identifier for this application is defined in Table 4.2.6.2.1.1-1.

3.3.4 Protocol data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

3.3.5 Procedures

3.3.5.1 Access Network Requirements

If the protocol receives an ***AddressManagement.SubnetChanged*** indication, the access network:

- May send a LocationRequest message to query the Location information.
- May send a LocationAssignment message to update the Location information.

3.3.5.2 Access Terminal Requirements

If the access terminal receives a LocationRequest message, it shall send LocationResponse message. If the access terminal's current stored LocationValue is not NULL, the access terminal shall set the LocationType, LocationLength, and LocationValue fields in this message to its stored values of these fields. If the access terminal's current stored LocationValue is equal to NULL, the access terminal shall omit the LocationType, LocationLength, and LocationValue fields in this message.

If the access terminal receives a LocationAssignment message, it shall send LocationComplete message as follows:

- If the access terminal's current stored Location is not NULL, the access terminal shall set the LocationType, LocationLength, and LocationValue fields of the LocationComplete message to its stored values of these fields. If the access terminal's current stored LocationValue is equal to NULL, the access terminal shall omit the LocationType, LocationLength, and LocationValue fields in this message
- The access terminal shall store the value of the LocationType, LocationLength, and LocationValue fields of the LocationAssignment message in LocationType, LocationLength, and LocationValue variables, respectively.

The access terminal shall set LocationValue to NULL if it receives ***SessionManagement.SessionClosed*** indication.

3.3.6 Message Formats

3.3.6.1 LocationRequest

The access network uses this message to query the access terminal of its Location information.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access network shall set this field to 0x03.

TransactionID The access network shall increment this value for each new LocationRequest message sent.

Channels	CC	FTC
Addressing		unicast

SLP	Best Effort
Priority	40

3.3.6.2 LocationResponse

The access terminal sends the LocationResponse message in response to the LocationRequest message.

Field	Length (bits)
MessageID	8
TransactionID	8
LocationType	8
LocationLength	0 or 8
LocationValue	0 or 8 × LocationLength

MessageID The access terminal shall set this field to 0x04.

TransactionID The access terminal shall set this field the TransactionID field of the corresponding LocationRequest message.

LocationType The access terminal shall set this field to 0 if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationType.

LocationLength The access terminal shall not include this field if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationLength.

LocationValue The access terminal shall not include this field if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationValue.

Channels	AC	RTC
Addressing		unicast

SLP	Reliable[1]	Best Effort
Priority	40	

3.3.6.3 LocationAssignment

The access network uses this message to update the Location information of the access terminal.

[1] This message is sent reliably when it is sent over the Reverse Traffic Channel.

Field	Length (bits)
MessageID	8
TransactionID	8
LocationType	8
LocationLength	8
LocationValue	8 × LocationLength

MessageID The access network shall set this field to 0x05.

TransactionID The access network shall increment this value for each new LocationAssignment message sent.

LocationType The access network shall set this field to the type of the location as specified in Table 3.3.6.3-1.

Table 3.3.6.3-1. LocationType Encoding

LocationType	LocationLength	Meaning
0x01	0x05	Location compatible with [3] (see Table 3.3.6.3-2)
All other values	N/A	Reserved

LocationLength The access network shall set this field to the length of the LocationValue field in octets as specified in Table 3.3.6.3-1.

LocationValue The access network shall set this field to the Location of type specified by LocationType. If LocationType is set to 0x01, the access network shall set this field as shown in Table 3.3.6.3-2, where SID, NID, and PACKET_ZONE_ID correspond to the current access network.

Table 3.3.6.3-2. Subfields of LocationValue when LocationType = 0x01

Sub-fields of LocationValue	# of bits
SID	15
Reserved	1
NID	16
PACKET_ZONE_ID	8

Channels	CC	FTC
Addressing		unicast

SLP	Best Effort
Priority	40

3.3.6.4 LocationComplete

The access terminal sends this message in response to the LocationAssignment message.

Field	Length (bits)
MessageID	8
TransactionID	8
LocationType	8
LocationLength	0 or 8
LocationValue	0 or 8 × LocationLength

MessageID The access terminal shall set this field to 0x06.

TransactionID The access terminal shall set this field the TransactionID field of the corresponding LocationAssignment message.

LocationType The access terminal shall set this field to 0 if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationType.

LocationLength The access terminal shall not include this field if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationLength.

LocationValue The access terminal shall not include this field if the value of its stored LocationValue is NULL; otherwise, the access terminal shall set this field to the stored value of LocationValue.

Channels	AC	RTC
Addressing		unicast

SLP	Reliable[2]	Best Effort
Priority	40	

3.3.7 Configuration Attributes

The following complex attribute and default values are defined (see 10.3 for attribute record definition):

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A
One or more of the following record:		
ValueID	8	N/A
PDSNSelectionType	8	0x00
PDSNSelectionDataLength	8	0x00
PDSNSelectionData	PDSNSelectionDataLength × 8	N/A

Length — Length of the complex attribute in octets. The access terminal shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — The access terminal shall set this field to 0x01.

ValueID — The access terminal shall set this field to an identifier assigned to this complex value.

PDSNSelectionType — The access terminal shall set this field to the type of the PDSN selection as shown in Table 3.3.7-1.

[2] This message is sent reliably when it is sent over the Reverse Traffic Channel.

Table 3.3.7-1. Encoding of PDSNSelectionType

PDSNSelectionType	Meaning
0x00	The access terminal does not provide the PDSNSelectionData.
0x01	PDSN selection as specified in [9]
All other values	Reserved

PDSNSelectionDataLength

The access terminal shall set this field to the length of the data provided for PDSN selection as shown in Table 3.3.7-2.

Table 3.3.7-2. Encoding of PDSNSelectionType, PDSNSelectionDataLength, and PDSNSelectionData

PDSNSelectionType	PDSNSelectionDataLength (octets)	PDSNSelectionData
0x00	0x00	N/A
0x01	0x08	IMSI

PDSNSelectionData The access terminal shall set this field to the data needed for PDSN selection with the type specified by PDSNSelectionType as shown in Table 3.3.7-2.

3.3.8 Interface to Other Protocols

3.3.8.1 Commands

This protocol does not issue any commands.

3.3.8.2 Indications

This protocol registers to receive the following indications:

- *AddressManagement.Closed*
- *AddressManagement.SubnetChanged*

No text.

3.4 Flow Control Protocol

3.4.1 Overview

The Flow Control Protocol provides procedures and messages used by the access terminal and the access network to perform flow control for the Default Packet Application Protocol.

This protocol can be in one of the following states:

- Close State: in this state the Default Packet Application does not send or receive any RLP packets.
- Open State: in this state the Default Packet Application can send or receive RLP packets.

Figure 3.4.1-1 and Figure 3.4.1-2 show the state transition diagram at the access terminal and the access network.

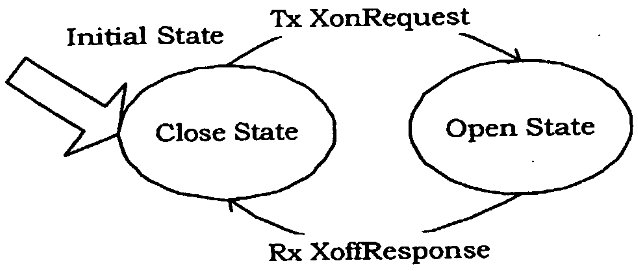


Figure 3.4.1-1. Flow Control Protocol State Diagram (Access Terminal)

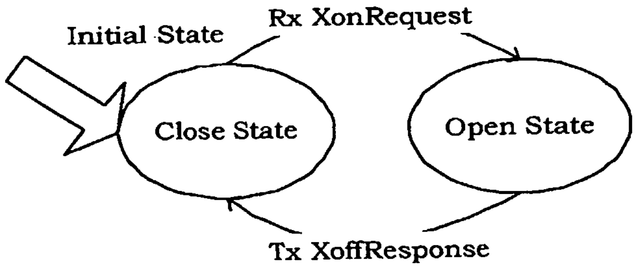


Figure 3.4.1-2. Flow Control Protocol State Diagram (Access Network)

3.4.2 Primitives and Public Data

3.4.2.1 Commands

This protocol does not define any commands.

3.4.2.2 Return Indications

This protocol does not return any indications.

3.4.2.3 Public Data

- None.

3.4.3 Basic Protocol Numbers

Flow Control Protocol is a protocol associated with the Default Packet Application. The application identifier for this application is defined in Table 4.2.6.2.1.1-1.

3.4.4 Protocol data Unit

The transmission unit of this protocol is a message. This is a control protocol and, therefore, it does not carry payload on behalf of other layers or protocols.

3.4.5 Procedures

3.4.5.1 Transmission and Processing of DataReady Message

The access network may send a DataReady message to indicate that there is data corresponding to this packet application awaiting to be transmitted.

The access terminal shall send a DataReadyAck within the time period specified by $T_{FCResponse}$ of reception of the DataReady message to acknowledge reception of the message.

3.4.5.2 Close State

In this state, the access terminal and the access network shall not send or receive any RLP packets.

3.4.5.2.1 Access Terminal Requirements

The access terminal shall send an XonRequest message when it is ready to exchange RLP packets with the access network. The access terminal should send an XonRequest message when it receives a DataReady from the access network.

The access terminal shall transition to the Open state when it sends an XonRequest message.

3.4.5.2.2 Access Network Requirements

If the access network receives an XonRequest message, it shall

- Send an XonResponse message within the time period specified by $T_{FCResponse}$ of reception of the XonRequest message to acknowledge reception of the message.
- Transition to the Open State.

3.4.5.3 Open State

In this state, the access terminal and the access network may send or receive any RLP packets.

3.4.5.3.1 Access Terminal Requirements

The access terminal may re-send an XonRequest message if it does not receive an XonResponse message an RLP packet within the time period specified by $T_{FCResponse}$ of sending the XonRequest message.

The access terminal may send an XoffRequest message to request the access network to stop sending RLP packets. The access terminal shall transition to the Close state when it receives an XoffResponse message.

The access terminal may re-send an XoffRequest message if it does not receive an XoffResponse message within the time period specified by $_{FCResponse}$ of sending the XoffRequest message.

3.4.5.3.2 Access Network Requirements

If the access network receives an XoffRequest message, it shall

- Send an XoffResponse message within the time period specified by $T_{FCResponse}$ of reception of XoffRequest message to acknowledge reception of the message.
- Transition to the Close State.

3.4.6 Message Formats

3.4.6.1 XonRequest

The access terminal sends this message to request transition to the Open State.

Field	Length (bits)
MessageID	8

MessageID The access terminal shall set this field to 0x07.

Channels	AC RTC	SLP	Best Effort
Addressing	unicast	Priority	40

3.4.6.2 XonResponse

The access network sends this message to acknowledge reception of the XonRequest message.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x08.

Channels	CC FTC
Addressing	unicast

SLP	Best Effort
Priority	40

3.4.6.3 XoffRequest

The access terminal sends this message to request transition to the Close State.

Field	Length (bits)
MessageID	8

MessageID The access terminal shall set this field to 0x09.

Channels	AC RTC
Addressing	unicast

SLP	Best Effort
Priority	40

3.4.6.4 XoffResponse

The access network sends this message to acknowledge reception of the XoffRequest message.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x0a.

Channels	CC FTC
Addressing	unicast

SLP	Best Effort
Priority	40

3.4.6.5 DataReady

The access network sends this message to indicate that there is data corresponding to this packet application awaiting to be transmitted.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access network shall set this field to 0x0b.

TransactionID The access network shall increment this value for each new DataReady message sent.

Channels	CC	FTC
Addressing		unicast

SLP	Best Effort
Priority	40

3.4.6.6 DataReadyAck

The access terminal sends this message to acknowledge reception of a DataReady message.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access terminal shall set this field to 0x0c.

TransactionID The access terminal shall set this value to the value of the TransactionID field of the corresponding DataReady message.

Channels	AC	RTC
Addressing		unicast

SLP	Best Effort
Priority	40

3.5 Configuration Messages

The Default Packet Application uses the Generic Configuration Protocol for configuration of the attribute listed in 3.3.7.

3.5.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for the Default Packet Application. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC
Addressing	unicast

SLP	Reliable
Priority	40

3.5.2 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

Channels	FTC RTC
Addressing	unicast

SLP	Reliable
Priority	40

No text.

4 STREAM LAYER

4.1 Introduction

4.1.1 General Overview

The Stream Layer provides the following functions:

- Multiplexing of application streams for one access terminal. Stream 0 is always assigned to the Signaling Application. The other streams can be assigned to applications with different QoS (Quality of Service) requirements, or other applications.
- Provision of configuration messages that map applications to streams.

The Stream Layer uses the Stream Layer Protocol to provide these functions.

4.1.2 Data Encapsulation

Figure 4.1.2-1 illustrates the relationship between an Application Layer packet, a Stream Layer packet and a Session Layer payload.

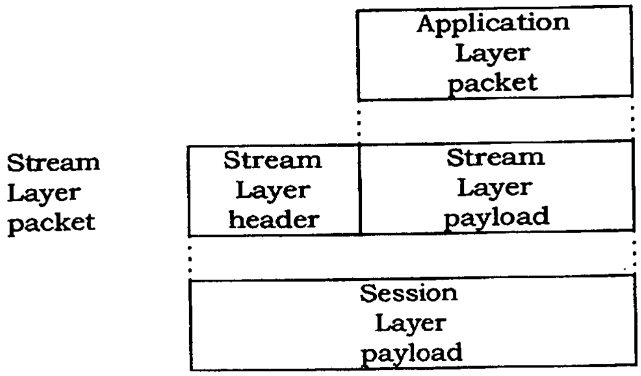


Figure 4.1.2-1. Stream Layer Encapsulation

4.2 Default Stream Protocol

4.2.1 Overview

The Default Stream Protocol provides the Stream Layer functionality. This protocol provides the ability to multiplex up to 4 application streams. Stream 0 is always reserved for a Signaling Application, and, by default, is assigned to the Default Signaling Application. By default, Stream 1 is assigned to the Default Packet Application.

This protocol uses the Generic Configuration Protocol (see 10.7) to define the format and processing of the configuration messages that map applications to streams.

The header added by this protocol is 2 bits in length. If x bits is the length of the payload presented to the Stream Layer, x shall satisfy

$$x \text{ modulo } 8 = 6.$$

4.2.2 Primitives and Public Data

4.2.2.1 Commands

This protocol does not define any commands.

4.2.2.2 Return Indications

This protocol does not return any indications.

4.2.2.3 Public Data

- None.

4.2.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{STRType}$.

The Subtype field for this protocol is two octets set to $N_{STRDefault}$.

4.2.4 Protocol Data Unit

The protocol data unit for this protocol is a Stream Layer Packet.

This protocol receives application packets for transmission from up to four different applications. The protocol adds the Stream header defined in 4.2.6.1 in front of each application packet and forwards it for transmission to the Session Layer.

All Stream Layer packets forwarded to the Session Layer shall be octet aligned.

The protocol receives Stream Layer packets from the Session Layer and removes the Stream Layer header. The application packet obtained in this manner is forwarded to the application indicated by the Stream field of the Stream Layer header.

The structure of the Stream Layer packet is shown in Figure 4.2.4-1

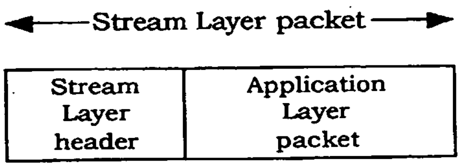


Figure 4.2.4-1. Stream Layer Packet Structure

4.2.5 Procedures

The access terminal and the access network may use the ConfigurationRequest and ConfigurationResponse messages to select the applications carried by each stream. When the access terminal and the access network use these messages, they shall process them according to the requirements presented in the Generic Configuration Protocol (see 10.7).

Applications can be mapped to the different streams during the AT Initiated State of the Session Configuration Protocol (see 5.4.5.5) as well as during the AN Initiated State of that protocol (see 5.4.5.6).

The ConfigurationRequest and ConfigurationResponse messages may be exchanged only when the session is set-up. The StreamConfiguration attribute and the default values for this attribute are presented in 4.2.6.2.1.1.

4.2.6 Header and Message Formats

4.2.6.1 Stream Header

The sender adds the following header in front of every Stream Layer payload (application packet):

Field	Length(bits)
Stream	2

Stream The sender shall set this field to the stream number associated with the application sending the application packet following the header.

4.2.6.2 Configuration Messages

The Default Stream Protocol uses the Generic Configuration Protocol to associate an application with a particular stream. The following messages are defined:

4.2.6.2.1 ConfigurationRequest

The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x50.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

The following complex attribute and default values are defined (see 10.3 for attribute record definition):

4.2.6.2.1.1 StreamConfiguration

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A
One or more of the following record:		
ValueID	8	N/A
Stream0Application	16	0x0000
Stream1Application	16	0xFFFF
Stream2Application	16	0xFFFF
Stream3Application	16	0xFFFF

Length — Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — The sender shall set this field to 0x00.

ValueID — The sender shall set this field to an identifier assigned to this complex value.

Stream0Application — The sender shall set this field to the identifier of the application used over Stream 0.

Stream1Application — The sender shall set this field to the identifier of the application used over Stream 1.

Stream2Application — The sender shall set this field to the identifier of the application used over Stream 2.

Stream3Application — The sender shall set this field to the identifier of the application used over Stream 3.

Sender shall set the last four fields to one of the non-reserved values in Table 4.2.6.2.1.1-1.

Table 4.2.6.2.1.1-1. Application Subtypes

Value	Meaning
0x0000	Default Signaling Application
0x0001	Default Packet Application bound to the access network.
0x0002	Default Packet Application bound to the service network.
0xFFFF	Stream not used
All other values are reserved.	

4.2.6.2.2 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the responder includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response and the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

4.2.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{STRType}$	Type field for this protocol.	Table 2.3.6-1
$N_{STRDefault}$	Subtype field for this protocol	0x0000

4.2.8 Interface to Other Protocols

4.2.8.1 Commands

This protocol does not issue any commands.

4.2.8.2 Indications

This protocol does not register to receive any indications.

No text.

5 SESSION LAYER

5.1 Introduction

5.1.1 General Overview

The Session Layer contains protocols used to negotiate a session between the access terminal and the access network.

A session is a shared state maintained between the access terminal and the access network, including information such as:

- A unicast address (UATI) assigned to the access terminal,
- the set of protocols used by the access terminal and the access network to communicate over the air-link,
- configuration settings for these protocols (e.g., authentication keys, parameters for Connection Layer and MAC Layer protocols, etc.), and
- an estimate of the current access terminal location.

During a single session the access terminal and the access network can open and close a connection multiple times; therefore, sessions will be closed rarely, and only on occasions such as the access terminal leaving the coverage area or such as prolonged periods in which the access terminal is unavailable.

The Session Layer contains the following protocols:

- Session Management Protocol: This protocol provides the means to control the activation of the other Session Layer protocols. In addition, this protocol ensures the session is still valid and manages closing of the session.
- Address Management Protocol: This protocol specifies procedures for the initial UATI assignment and maintains the access terminal addresses.
- Session Configuration Protocol: This protocol provides the means to negotiate and provision the protocols used during the session, and negotiates the configuration parameters for these protocols. This protocol uses the procedures and attribute-value formats defined by the Generic Configuration Protocol (see 10.7) for protocol negotiation.

The relationship between the Session Layer protocols is illustrated in Figure 5.1.1-1.

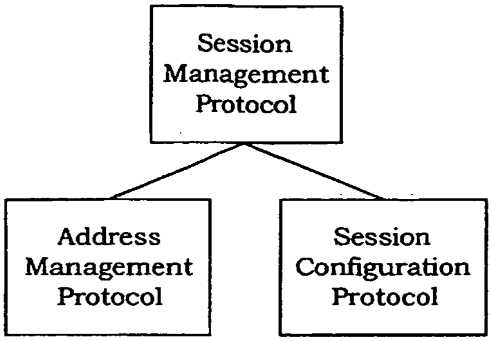

Session Management Protocol
Address Management Protocol
Session Configuration Protocol

Figure 5.1.1-1. Session Layer Protocols

5.1.2 Data Encapsulation

The Session Layer does not modify transmitted or received packets.

Figure 5.1.2-1 illustrates the relationship between Stream Layer packets, Session Layer packets, and Connection Layer payload.

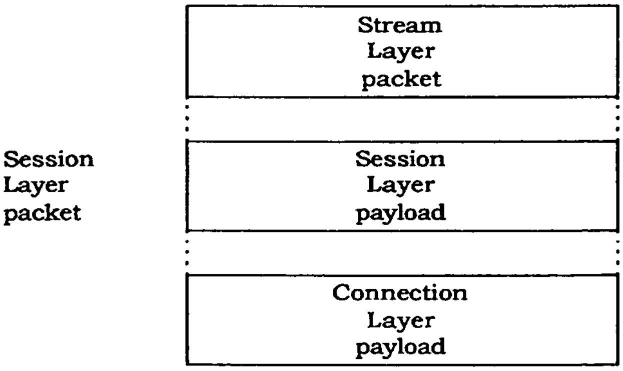


Figure 5.1.2-1. Session Layer Encapsulation

5.2 Default Session Management Protocol

5.2.1 Overview

The Default Session Management protocol provides the means to control the activation of the Address Management Protocol and then the Session Configuration Protocol, in that order, before a session is established. This protocol also periodically ensures that the session is still valid and manages closing the session.

The actual behavior and message exchange in each state of this protocol are mainly governed by protocols that are activated by the Default Session Management Protocol. These protocols return indications, which trigger the state transitions of this protocol.

This protocol can be in one of four states:

- Inactive State: This state applies only to the access terminal. In this state there are no communications between the access terminal and the access network.
- AMP Setup State: In this state the access terminal and access network perform exchanges governed by the Address Management Protocol and the access network assigns a UATI to the access terminal.
- Open State: In this state a session is open.
- Close State: This state applies only to the access network. In this state the access network waits for the close procedure to complete.

Figure 5.2.1-1 provides an overview of the access terminal states and state transitions.

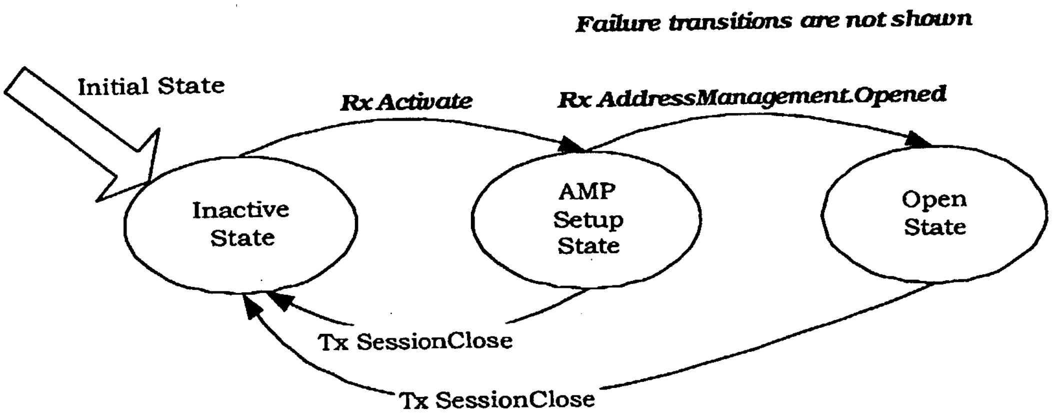


Figure 5.2.1-1. Session Management Protocol State Diagram (Access Terminal)

Figure 5.2.1-2 provides an overview of the access network states and state transitions.

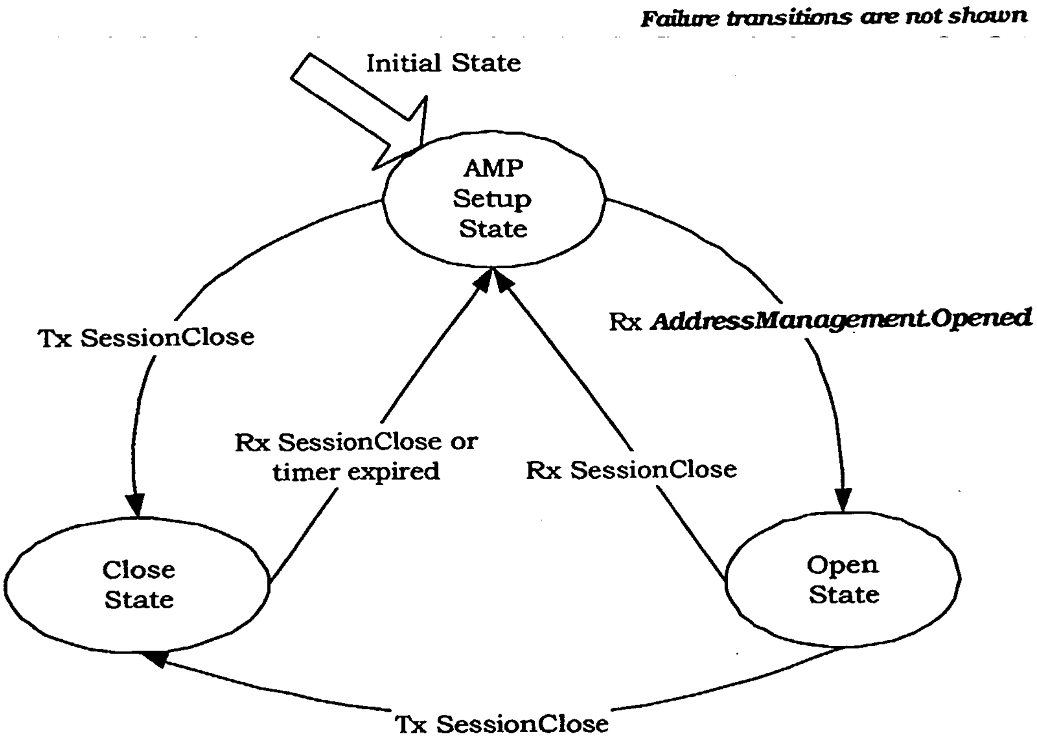

Failure transitions are not shown
Initial State
AMP Setup State
Tx SessionClose
Rx *AddressManagement.Opened*
Rx SessionClose or timer expired
Rx SessionClose
Close State
Open State
Tx SessionClose

Figure 5.2.1-2. Session Management Protocol State Diagram (Access Network)

5.2.2 Primitives and Public Data

5.2.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***

5.2.2.2 Return Indications

This protocol returns the following indications:

- ***BootCompleted***
- ***SessionOpened***
- ***SessionClosed***

5.2.2.3 Public Data

- None.

5.2.3 Basic Protocol Numbers

The Type field for the Session Management Protocol is one octet, set to $N_{SMPType}$.

The Subtype field for the Session Management Protocol is two octets, set to $N_{SMPDefault}$.

5.2.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

5.2.5 Procedures

5.2.5.1 Protocol Initialization

This protocol shall be started in the Inactive State for the access terminal.

This protocol shall be started in the Address Management Protocol (AMP) Setup State for the access network.

This protocol does not have any initial configuration requirements.

5.2.5.2 Command Processing

The list of events that causes an ***Activate*** or ***Deactivate*** command to be sent to this protocol is outside the scope of this specification.

5.2.5.2.1 Activate

If the access terminal receives the ***Activate*** command in the Inactive State, it shall transition to the AMP Setup State.

If the access terminal receives the ***Activate*** command in any state other than the Inactive State, the command shall be ignored.

The access network shall ignore the command.

5.2.5.2.2 Deactivate

If the access terminal receives a ***Deactivate*** command in the Inactive State, the command shall be ignored.

If the access terminal receives a ***Deactivate*** command in any state other than the Inactive State, the access terminal shall perform the following:

- Send a SessionClose message to the access network.
- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.

- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the Inactive State.

If the access network receives a ***Deactivate*** command in the Close State, the command shall be ignored.

If the access network receives a ***Deactivate*** command in any state other than the Close State, the access network shall send a SessionClose message and transition to the Close State.

5.2.5.3 Processing the SessionClose Message

If the access terminal receives a SessionClose message in the Inactive State, the message shall be ignored.

If the access terminal receives a SessionClose message in any state other than the Inactive State, the access terminal shall perform the following:

- Send a SessionClose message to the access network.
- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the Inactive State.

If the access network receives a SessionClose message in the Close State, the access network shall process it as specified in 5.2.5.8.

If the access network receives a SessionClose message in any state other than the Close State, the access network shall:

- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the AMP Setup State.

5.2.5.4 Processing Failure Indications

The access terminal shall ignore an ***AddressManagement.Failed***, or ***SessionConfiguration.Failed*** indication, if it receives it in the Inactive State.

If the access terminal receives an ***AddressManagement.Failed***, or ***SessionConfiguration.Failed*** indication while in any state other than the Inactive State, then the access terminal shall perform the following:

- Send a SessionClose message to the access network.
- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- The access terminal shall transition to the Inactive State.

If the access network receives an ***AddressManagement.Failed***,a or ***SessionConfiguration.Failed*** indication, the access network shall perform the following:

- Send a SessionClose message to the access terminal.
- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the AMP Setup State.

5.2.5.5 Inactive State

This state only applies to the access terminal. In this state there are no communications between the access terminal and the access network. The access terminal does not maintain any session-related state and the access network may be unaware of the access terminal's existence within its coverage area when the access terminal's Session Management Protocol is in this state.

5.2.5.6 AMP Setup State

In this state the Session Management Protocol in the access terminal sends an ***AddressManagement.Activate*** command to the Address Management Protocol and waits for the Address Management Protocol to respond.

5.2.5.6.1 Access Terminal Requirements

Upon entering the AMP Setup State, the access terminal shall send an ***AddressManagement.Activate*** command to the Address Management Protocol.

If the access terminal receives an ***AddressManagement.Opened*** indication, it shall perform the following:

- Issue a ***SessionConfiguration.Activate*** command.
- Return a ***BootCompleted*** indication.
- Transition to the Open State.

5.2.5.6.2 Access Network Requirements

If the access network receives an ***AddressManagement.Opened*** indication, it shall perform the following:

- Issue a ***SessionConfiguration.Activate*** command.
- Return a ***BootCompleted*** indication.
- Transition to the Open State.

5.2.5.7 Open State

In the Open State the access terminal has an assigned UATI and the access terminal and the access network have configured a session using the Session Configuration Protocol.

If the protocol receives a ***SessionConfiguration.SCPChangeda***indication, it shall issue ***SessionConfiguration.Activate*** command to the selected Session Configuration Protocol.

The access terminal and the access network shall support the keep-alive mechanism defined in 5.2.5.7.1.

5.2.5.7.1 Keep Alive Functions

The access terminal and the access network shall monitor the traffic flowing on the Forward Channel and Reverse Channel, respectively, directed to-or-from the access terminal. If either the access terminal or the access network detects a period of inactivity of at least $T_{SMPClose}/N_{SMPKeepAlive}$ minutes, it may send a KeepAliveRequest message. The recipient of the message shall respond by sending the KeepAliveResponse message. When a KeepAliveResponse message is received, the access terminal shall not send another KeepAliveRequest message for at least $T_{SMPClose}/N_{SMPKeepAlive}$ minutes.

If the access terminal does not detect any traffic from the access network directed to it for a period of at least $T_{SMPClose}$ minutes, it shall perform the following:

- Issue an ***AirlinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the Inactive State.

If the access network does not detect any traffic from the access terminal directed to it for a period of at least $T_{SMPClose}$ minutes, it should perform the following:

- Issue an ***AirlinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the AMP Setup State.

If the value of $T_{SMPClose}$ is set to zero, the access terminal and the access network shall not send or expect keep-alive messages, and shall disable the transitions occurring as a consequence of not receiving these messages.

5.2.5.8 Close State

The Close State is associated only with the protocol in the access network. In this state the protocol in the access network waits for a SessionClose message from the access terminal or an expiration of a timer.

The access network shall set the Close State timer upon entering this state. The value of this timer shall be set to $T_{SMPClose}$ or $T_{SMPMinClose}$, whichever is larger.

When the access network receives a SessionClose message or when the Close State timer expires the protocol shall:

- Issue an ***AirLinkManagement.CloseConnection*** command.
- Issue an ***AddressManagement.Deactivate*** command.
- Issue a ***SessionConfiguration.Deactivate*** command.
- Return a ***SessionClosed*** indication.
- Transition to the AMP Setup State.

If the access network receives any other Session Management Protocol message from the access terminal using the UATI assigned during this session, it shall discard the message.

5.2.6 Message Formats

5.2.6.1 SessionClose

The sender sends the SessionClose message to terminate the session.

Field	Length (bits)
MessageID	8
CloseReason	8
MoreInfoLen	8
MoreInfo	8 × MoreInfoLen

MessageID The sender shall set this field to 0x01.

CloseReason The sender shall set this field to the close reason as shown in Table 5.2.6.1-1

Table 5.2.6.1-1. Encoding of CloseReason Field

Field Value	Meaning	MoreInfoLen	MoreInfo
0x00	Normal Close	0	N/A
0x01	Close Reply	0	N/A
0x02	Protocol Error	0	N/A
0x03	Protocol Configuration Failure	3	Type followed by Subtype
0x04	Protocol Negotiation Error	variable	zero or more Type followed by Subtype followed by offending attribute records.
0x05	Session Configuration Failure	0	N/A
0x06	Session Lost	0	N/A
0x07	Session Unreachable	0	N/A
0x08	All session resources busy	0	N/A
All other values are reserved			

MoreInfoLen Length in octets of the MoreInfo field.

MoreInfo Additional information pertaining to the closure. The format of this field is determined by the particular close reason.

Channels	CC AC FTC RTC	SLP	Best Effort
Addressing	unicast	Priority	40

5.2.6.2 KeepAliveRequest

The sender sends the KeepAliveRequest to verify that the peer is still alive.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The sender shall set this field to 0x02.

TransactionID The sender shall increment this value for each new KeepAliveRequest message sent.

Channels	CC	AC	FTC	RTC
Addressing	unicast			

SLP	Best Effort
Priority	40

5.2.6.3 KeepAliveResponse

The sender sends the KeepAliveResponse message as an answer to the KeepAliveRequest message.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The sender shall set this field to 0x03.

TransactionID The sender shall set this value to the value of the TransactionID field of the corresponding KeepAliveRequest message.

Channels	CC	AC	FTC	RTC
Addressing	unicast			

SLP	Best Effort
Priority	40

5.2.6.4 Configuration Messages

The Default Session Management Protocol uses the Generic Configuration Protocol for configuration. All configuration messages sent by this protocol shall have their Type field set to $N_{SMPType}$.

The negotiable attributes for this protocol are listed in Table 5.2.6.4-1. The access terminal shall use as defaults the values in Table 5.2.6.4-1 typed in *bold italics*.

Table 5.2.6.4-1. Configurable Attributes

Attribute ID	Attribute	Values	Meaning
0xff	$T_{SMPClose}$	*0x0CA8*	Default is 54 hours.
		0x0000 to 0xFFFF	0x0000 means disable keep alive messages; all other values are in minutes.

5.2.6.4.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for the Session Management Protocol. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

5.2.6.4.2 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

5.2.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{SMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{SMPDefault}$	Subtype field for this protocol	0x0000
$N_{SMPKeepAlive}$	Maximum number of keep alive transactions wthin $T_{SMPClose}$.	3
$T_{SMPMinClose}$	Minimum recommended timer setting for Close State	300 seconds

5.2.8 Interface to Other Protocols

5.2.8.1 Commands Sent

This protocol issues the following commands:

- *AddressManagement.Activate*
- *SessionConfiguration.Activate*
- *AddressManagement.Deactivate*
- *SessionConfiguration.Deactivate*
- *AirLinkManagement.CloseConnection*

5.2.8.2 Indications

This protocol registers to receive the following indications:

- *AddressManagement.Failed*
- *SessionConfiguration.Failed*
- *AddressManagement.Opened*
- *SessionConfiguration.SCPChanged*

5.3 Default Address Management Protocol

5.3.1 Overview

The Default Address Management Protocol provides the following functions:

- Initial UATI assignment
- Maintaining the access terminal unicast addresse as the access terminal moves between subnets.

This protocol operates in one of three states:

- Inactive State: In this state there are no communications between the access terminal and the access network.
- Setup State: In this state the access terminal and the access network perform a UATIRequest/UATIAssignment/UATIComplete exchange to assign the access terminal a UATI.
- Open State: In this state the access terminal has been assigned a UATI. The access terminal and access network may also perform UATIRequest/UATIAssignmenta /UATIComplete or UATIAssignment/UATIComplete exchange so that the access terminal obtains a new UATI.

The protocol states and the messages and events causing the transition between the states are shown in Figure 5.3.1-1 and Figure 5.3.1-2.

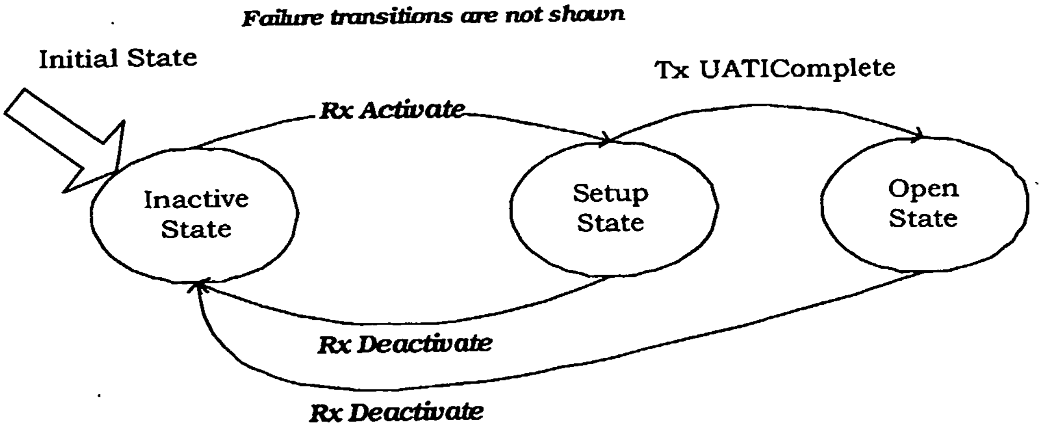


Figure 5.3.1-1. Address Management Protocol State Diagram (Access Terminal)

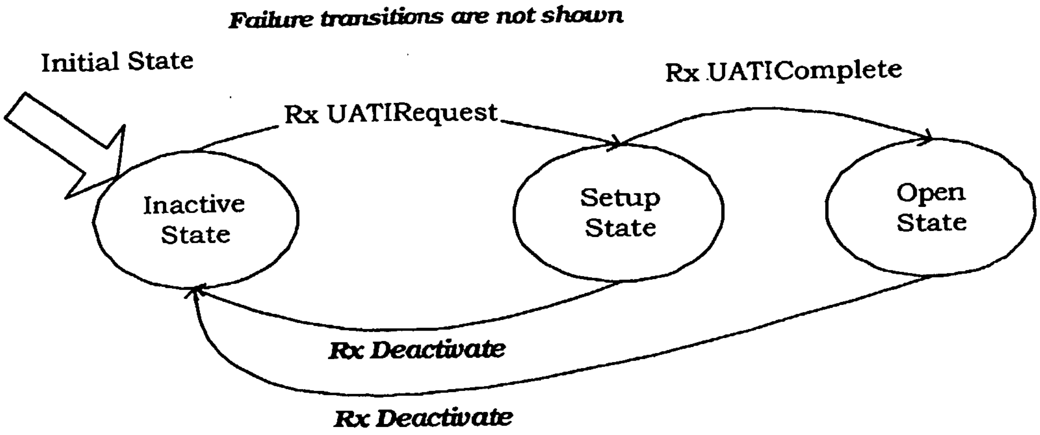


Figure 5.3.1-2. Address Management Protocol State Diagram (Access Network)

5.3.2 Primitives and Public Data

5.3.2.1 Commands

This protocol defines the following command:

- ***Activate***
- ***Deactivate***
- ***UpdateUATI***

5.3.2.2 Return Indications

This protocol returns the following indications:

- ***Opened***
- ***UATIReleased***
- ***UATIAssigned***
- ***Failed***
- ***SubnetChanged***

5.3.2.3 Public Data

- ReceiveATIList
- TransmitATI
- SessionSeed

5.3.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{ADMPType}$.

The Subtype field for this protocol is two octets set to $N_{ADMPDefault}$.

5.3.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

5.3.5 Procedures

5.3.5.1 Protocol Initialization

This protocol shall be started in the Inactive State.

This protocol does not have any initial configuration requirements.

5.3.5.2 Command Processing

5.3.5.2.1 Activate

If the protocol receives the ***Activate*** command in the Inactive State:

- The access terminal shall transition to the Setup State.
- The access network shall ignore the command.

If the protocol receives the ***Activate*** command in any state other than the Inactive State, the command shall be ignored.

5.3.5.2.2 Deactivate

If the protocol receives the ***Deactivate*** command in the Inactive State, the command shall be ignored.

If the protocol receives the ***Deactivate*** command in any state other than the Inactive State, the protocol shall transition to the Inactive State and return a ***UATIReleased*** indication.

5.3.5.2.3 UpdateUATI

The access network and access terminal shall ignore the ***UpdateUATI*** command when it is received in any state other than the Open State.

The access network shall send a UATIAssignment message when it receives an ***UpdateUATI*** command in the Open State.

The access terminal shall follow the procedures in 5.3.5.6.1.1 to send a UATIRequest message when it receives an ***UpdateUATI*** command in the Open State.

A comprehensive list of events causing the ***UpdateUATI*** command is beyond the scope of this specification.

5.3.5.3 UATIAssignment Message Validation

Each time that the access network sends a new UATIAssignment message, it shall increment the value of the MessageSequence field. If the access network is sending the same message multiple times, it shall not change the value of this field between transmissions.

The access terminal shall initialize a receive pointer for the UATIAssignment message validation, ***V(R)***, to 255 when it sends a UATIRequest message and ReceiveATIList[I_{RATI}].ATI is not set to NULL.

When the access terminal receives a UATIAssignment message, it shall validate the message, using the procedure defined in 10.6 (S is equal to 8). The access terminal shall discard the message if it is stale.

5.3.5.4 Processing HardwareIDRequest message

Upon reception of a HardwareIDRequest message, the access terminal shall respond with a HardwareIDResponse message. The access terminal shall set the HardwareID record of the HardwareIDResponse message to the unique ID that has been assigned to the terminal by the manufacturer.

5.3.5.5 Inactive State

In this state, there are no communications between the access terminal and the access network. The access terminal does not have an assigned UATI, the access network does not maintain a UATI for the access terminal, and may be unaware of the access terminal's existence within its coverage area.

5.3.5.5.1 Access Terminal Requirements

Upon entering the Inactive State, the access terminal shall perform the following:

- Set OldUATI to NULL.
- Set ReceiveATIList[I_{BATI}] to <ATIType = '00', ATI = NULL>.
- Set ReceiveATIList[$I_{currentUATI}$] to <ATIType = '10', ATI = NULL>.
- Set ReceiveATIList[$I_{newUATI}$] to <ATIType = '10', ATI = NULL>.
- Set ReceiveATIList[I_{RATI}] to <ATIType = '11', ATI = NULL>.
- Set TransmitATI to <ATIType = NULL, ATI = NULL>.
- Set UATI to NULL.
- Set UATIColorCode to NULL.

- Set UATISubnetMask to NULL.
- Set SessionSeed to the 32-bit pseudo-random number generated using output of the pseudo random number generator specified in 10.5.
- Disable the DualAddressTimer.

If the access terminal receives an ***Activate*** command, it shall transition to the Setup State.

5.3.5.5.2 Access Network Requirements

Upon entering the Inactive State, the access network shall perform the following:

- Set the value of the access terminal's UATI to NULL.
- Set the value of the access terminal's UATISubnetMask to NULL.
- Set the value of the access terminal's UATIColorCode to NULL.

The access network shall transition to the Setup State if it receives a UATIRequest message.

5.3.5.6 Setup State

In this state, the access terminal sends a request to the access network asking for a UATI and waits for the access network's response.

5.3.5.6.1 Access Terminal Requirements

Upon entering the Setup State the access terminal shall perform the following:

- Set the TransmitATI to
  <ATIType = '11', ATI = SessionSeed>,
- Set ReceiveATIList[I_{RATI}] to
  <ATIType = '11', ATI = SessionSeed>.
- Shall follow the procedures in 5.3.5.6.1.1 for sending a UATIRequest message.

A valid (see 5.3.5.3) UATIAssignment message that satisfies either of the following conditions is called a "fresh" UATIAssignment message:

- OverheadParametersUpToDate, provided as the public data of the Overhead Messages Protocol, is equal to 1 and the UATIColorCode field in the message matches the ColorCode, given as public data of the Overhead Messages Protocol, or
- the SubnetIncluded field of the message is equal to '1',

The access terminal shall discard a UATIAssignment message that is not "fresh".

If the access terminal does not receive a "fresh" UATIAssignment message within $T_{ADMPATResponse}$ seconds after receiving an ***AccessChannelMAC.TxEnded*** indication, it shall return a ***Failed*** indication and transition to the Inactive State.

If the access terminal receives a "fresh" UATIAssignment message then the access terminal shall perform the following:

- Set the UATIColorCode to the UATIColorCode given in the message.
- Set its UATI and UATISubnetMask as follows:
  - If the message includes the UATI104 field and UATISubnetMask field, the access terminal shall set its UATI to UATI104 | UATI024 and UATISubnetMask to UATISubnetMask field included in the message.
  - Otherwise, the access terminal shall set its UATI to (SectorID[127:24] | UATI024) and UATISubnetMask to SubnetMask where SectorID and SubnetMask are provided as public data of Overhead Messages Protocol.
- Set ReceiveATIList[I_{RATI}] to <ATIType = '11', ATI = NULL>.
- Set ReceiveATIList[$I_{currentUATI}$] to <ATIType = '10', ATI = (UATIColorCode | UATI[23:0])>.
- Set the TransmitATI to <ATIType = '10', ATI = (UATIColorCode | UATI[23:0])>.
- Return an ***Opened*** indication.
- Return a ***UATIAssigned*** indication.
- Send a UATIComplete message.
- Transition to the Open State.

5.3.5.6.1.1 Procedures for Sending a UATIRequest message

The access terminal shall follow the following procedures for sending a UATIRequest message:

- If OverheadParametersUpToDate, given as public data by the Overhead Messages Protocol, is equal to 0, the access terminal shall wait until it receives an ***OverheadMessages.Updated*** indication before it sends a UATIRequest message.
- Otherwise, the access terminal shall send a UATIRequest message without waiting for an ***OverheadMessages.Updated*** indication.

5.3.5.6.2 Access Network Requirements

When the access network sends a UATIAssignment message, it shall perform the following:

- Access network shall assign a Unicast Access Terminal Identifier (UATI) to the access terminal for the session as follows:
  - Access network may include both UATI104 and UATISubnetMask fields in the UATIAssignment message.

  - Access network may omit the UATI104 and UATISubnetMask fields from the message. In this case, the UATI[127:24] is implicitly assigned to be equal to SectorID[127:24] and UATISubnetMask is implicitly assigned to be SubnetMask, where SectorID and SubnetMask correspond to the sector that has received the UATIRequest message.

When the access network receives the corresponding UATIComplete message with the MessageSequence field of the UATIAssignment message sent, it shall perform the following:

- Return ***Opened*** indication.
- Return ***UATIAssigned*** indication.
- Transition to Open State.

If the access network does not receive the corresponding UATIComplete message in response to the UATIAssignment message, it may re-transmit the UATIAssignment message.

5.3.5.7 Open State

In this state the access terminal has been assigned a UATI.

5.3.5.7.1 Access Terminal Requirements

If the access terminal receives a ***RouteUpdate.IdleHO*** indication, and if either of the following two conditions is true, it shall set OldUATI to UATI and follow the procedures in 5.3.5.6.1.1 for sending a UATIRequest message:

- The UATISubnetMask is not equal to the SubnetMask of the sector in the active set, or
- The result of bitwise logical AND of the UATI and its subnet mask specified by UATISubnetMask is different from the result of bitwise logical AND of SectorID and its subnet mask specified by SubnetMask (where SectorID and SubnetMask correspond to the sector in the active set).

Also, if the access terminal receives a ***UpdateUATI*** command, it shall set OldUATI to UATI and follow the procedures in 5.3.5.6.1.1 for sending a UATIRequest message.

A valid (see 5.3.5.3) UATIAssignment message that satisfies either of the following conditions is called a “fresh” UATIAssignment message:

- OverheadParametersUpToDate, provided as the public data of the Overhead Messages Protocol, is equal to 1 and the UATIColorCode field in the message matches the ColorCode, given as public data of the Overhead Messages Protocol, or
- the SubnetIncluded field of the message equal to ‘1’,

The access terminal shall discard a UATIAssignment message that is not “fresh”.

If the access terminal does not receive a "fresh" UATIAssignment message within $T_{ADMPATResponse}$ seconds after receiving an ***AccessChannelMAC.TxEnded*** indication, it shall return a ***Failed*** indication and transition to the Inactive State.

If the access terminal receives a "fresh" UATIAssignment message then the access terminal shall perform the following:

- Set the UATIColorCode to the UATIColorCode given in the message.
- Set its UATI and UATISubnetMask as follows:
  - If the message includes the UATI104 field and UATISubnetMask field, the access terminal shall set its UATI to UATI104 | UATI024 and UATISubnetMask to UATISubnetMask field included in the message.
  - Otherwise, the access terminal shall set its UATI to (SectorID[127:24] | UATI024) and UATISubnetMask to SubnetMask where SectorID and SubnetMask are provided as public data of Overhead Messages Protocol.
- Set ReceiveATIList[$I_{newUATI}$] to <ATIType = '10', ATI = (UATIColorCode | UATI[23:0])>.
- Set the TransmitATI to <ATIType = '10', ATI = (UATIColorCode | UATI[23:0])>.
- Return a ***UATIAssigned*** indication.
- Send a UATIComplete message.
- Reset and start the DualAddress timer with a timeout value of $T_{ADMPDualAddress}$.

The access terminal shall perform the following when the DualAddress timer expires:

- Disable the DualAddress timer.
- Set ReceiveATIList[$I_{currentUATI}$] to ReceiveATIList[$I_{newUATI}$].

If the access terminal receives an ***InitializationState.NetworkAcquired*** indication and determines that either of the two following conditions is true, it shall return a ***Failed*** indication and transition to the Inactive State:

- The UATISubnetMask is not equal to the SubnetMask of the sector in the active set, or
- The result of bitwise logical AND of the UATI and its subnet mask specified by UATISubnetMask is different from the result of bitwise logical AND of SectorID and its subnet mask specified by SubnetMask (where SectorID and SubnetMask correspond to the sector in the active set).

5.3.5.7.2 Access Network Requirements

The access network may send a UATIAssignment message at any time in this state. The access network may send a UATIAssignment message if it receives ***RouteUpdate.ActiveSetUpdated*** indication, if it receives a ***UATIUpdate*** command, or in response to a UATIRequest message.

The access network may return a ***SubnetChanged*** indication and send a UATIAssignment message after reception of a ***RouteUpdate.ActiveSetUpdated*** indication. The triggers for returning a ***SubnetChanged*** indication after reception of a ***RouteUpdate.ActiveSetUpdated*** indication are outside the scope of this specification.

When the access network sends a UATIAssignment message, it shall perform the following:

- Assign a Unicast Access Terminal Identifier (UATI) to the access terminal for the session and include it in a UATIAssignment message.
  - If the UATIAssignment message is sent in response to a UATIRequest message, the access network may include both UATI104 and UATISubnetMask. If the access network does not include the UATI104 and UATISubnetMask fields in the message, the UATI[127:24] is implicitly assigned to be equal to SectorID[127:24], where SectorID corresponds to the sector that has received the UATIRequest message.
  - Otherwise, the access network shall include both UATI104 and UATISubnetMask fields in the UATIAssignment message.

When the access network receives a UATIComplete message with the MessageSequence field that is equal to the MessageSequence field of the UATIAssignment message that it has sent, it shall return a ***UATIAssigned*** indication.

If the access network does not receive the UATIComplete message in response to the corresponding UATIAssignment message within a certain time interval that is specified by the access network[3], it should re-transmit the UATIAssignment message.

5.3.6 Message Formats

5.3.6.1 UATIRequest

The access terminal sends the UATIRequest message to request that a UATI be assigned or re-assigned to it by the access network.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access terminal shall set this field to 0x00.

TransactionID The access terminal shall increment this value modulo 256 for each new UATIRequest message sent.

[3] The value of this timeout is determined by the access network and specification f the timeout value is outside the scope of this document.

Channels	AC	SLP	Best Effort
Addressing	unicast	Priority	10

5.3.6.2 UATIAssignment

The access network sends the UATIAssignment message to assign or re-assign a UATI to the access terminal.

Field	Length (bits)
MessageID	8
MessageSequence	8
Reserved1	7
SubnetIncluded	1
UATISubnetMask	0 or 8
UATI104	0 or 104
UATIColorCode	8
UATI024	24
UpperOldUATILength	4
Reserved2	4

MessageID — The access network shall set this field to 0x01.

MessageSequence — The access network shall set this to 1 higher than the MessageSequence field of the last UATIAssignment message (modulo 256) that it has sent to this access terminal.

Reserved1 — The access network shall set this field to zero. The access terminal shall ignore this field.

SubnetIncluded — The access network shall set this field to '1' if the UATI104 field and UATISubnetMask fields are included in this message; otherwise, the access network shall set this field to '0'.

UATISubnetMask — The access network shall omit this field if SubnetIncluded is set to '0'. If included, the access network shall set this field to the number of consecutive 1's in the subnet mask of the subnet to which the assigned UATI belongs.

UATI104 The access network shall omit this field if SubnetIncluded is set to '0'. If included, the access network shall set this field to UATI[127:24] of the UATI that it is assigning to the access terminal.

UATIColorCode UATI Color Code. The access network shall set this field to the Color Code associated with the subnet to which the UATI belongs.

UATI024 The access network shall set this field to UATI[23:0] of the UATI that it is assigning to the access terminal.

UpperOldUATILength The access network shall set this field the number of least significant bytes of OldUATI[127:24] that the access terminal is to send in the UATIComplete message.

Reserved2 The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC FTC	SLP	Best Effort
Addressing	unicast	Priority	10

5.3.6.3 UATIComplete

The access terminal sends this message to notify the access network that it has received the UATIAssignment message.

Field	Length (bits)
MessageID	8
MessageSequence	8
Reserved	4
UpperOldUATILength	4
UpperOldUATI	8 × UpperOldUATILength

MessageID The access terminal shall set this field to 0x02.

MessageSequence The access terminal shall set this field to the MessageSequence field of the UATIAssignment message whose receipt this message is acknowledging.

Reserved The access terminal shall set this field to zero. The access network shall ignore this field.

UpperOldUATILength The access terminal shall set this field to the length of the UpperOldUATI field in octets.

UpperOldUATI If UpperOldUATILength in the UATIAssignment message whose receipt this message is acknowledging is not zero and OldUATI is not NULL, the access terminal shall set this field to OldUATI[23+UpperOldUATILength×8:24]. Otherwise, the access terminal shall omit this field.

Channels	AC RTC	SLP	Reliable[4] Best Effort
Addressing	unicast	Priority	10

5.3.6.4 HardwareIDRequest

The access network uses this message to query the access terminal of its Hardware ID information.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access network shall set this field to 0x03.

TransactionID The access network shall increment this value for each new HardwareRequest message sent.

Channels	CC FTC	SLP	Best Effort
Addressing	unicast	Priority	40

5.3.6.5 HardwareIDResponse

The access terminal sends this message in response to the HardwareIDRequest message.

[4] This message is sent reliably when it is sent over the Reverse Traffic Channel.

Field	Length (bits)
MessageID	8
TransactionID	8
HardwareIDType	24
HardwareIDLength	8
HardwareIDValue	8×HardwareIDLength

MessageID The access terminal shall set this field to 0x04.

TransactionID The access terminal shall set this field the TransactionID field of the corresponding HardwareIDRequest message.

HardwareIDType The access terminal shall set this field according to Table 5.3.6.5-1.

Table 5.3.6.5-1. HardwareIDType encoding

HardwareIDType field value	Meaning
0x010000	Electronic Serial Number (ESN)
0x00NNNN	Hardware ID "NNNN" from [8]
0xFFFFFF	Null
All other values	Invalid

HardwareIDLength If HardwareIDType is not set to 0xFFFFFF, the access terminal shall set this field to the length in octets of the HardwareIDValue field; otherwise the access terminal shall set this field to 0x00.

HardwareIDValue The access terminal shall set this field to the unique ID (specified by HardwareIDType) that has been assigned to the terminal by the manufacturer.

Channels	AC	RTC

SLP	Reliable[5]	Best Effort

[5] This message is sent reliably when it is sent over the Reverse Traffic Channel.

Addressing	unicast

Priority	40

5.3.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{ADMPType}$	Type field for this protocol.	Table 2.3.6-1
$N_{ADMPDefault}$	Subtype field for this protocol	0x0000
$T_{ADMPATResponse}$	Time to receive UATIAssignment after sending UATIRequest	120 seconds
$T_{ADMPDualAddress}$	The duration of time that the access terminal declares an address match if it receives a message that is addressed using either the old or the new UATI	180 seconds

5.3.8 Interface to Other Protocols

5.3.8.1 Commands

This protocol does not issue any commands.

5.3.8.2 Indications

This protocol registers to receive the following indications:

- ***RouteUpdate.IdleHO***
- ***RouteUpdate.ActiveSetUpdated***
- ***InitializationState.NetworkAcquired***
- ***OverheadMessages.Updated***

5.4 Default Session Configuration Protocol

5.4.1 Overview

The Default Session Configuration Protocol provides for the negotiation and configuration of the set of protocols used during a session.

This protocol supports two phases of negotiation:

- Access terminal initiated negotiation: In this phase negotiation exchanges are initiated by the access terminal. This phase is used to negotiate the protocols that will be used in the session and negotiate some of the protocols' parameters (e.g., authentication key lengths).
- Access network initiated negotiation: In this phase negotiation exchanges are initiated by the access network. This phase is typically used to override default values used by the negotiated protocols.

This protocol uses the Generic Configuration Protocol procedures and messages when performing the negotiation in each phase (see 10.7). Even if the access terminal requires the use of a Session Configuration Protocol other than the Default Session Configuration Protocol, it shall use the Default Session Configuration Protocol to negotiate the other Session Configuration Protocol.

Example message flow diagrams for an extensive negotiation initiated by the access terminal and a minimal negotiation initiated by the access network are shown in 5.4.9.

Additional protocols may be negotiated without further modifications to the Default Session Configuration Protocol.

This protocol operates in one of four states:

- Inactive State: In this state, the protocol waits for an ***Activate*** command.
- AT Initiated State: In this state, negotiation is performed at the initiative of the access terminal.
- AN Initiated State: In this state, negotiation is performed at the initiative of the access network.
- Open State: In this state, the access terminal may initiate the session configuration procedure at any time and the access network may request the access terminal to initiate the session configuration at any time.

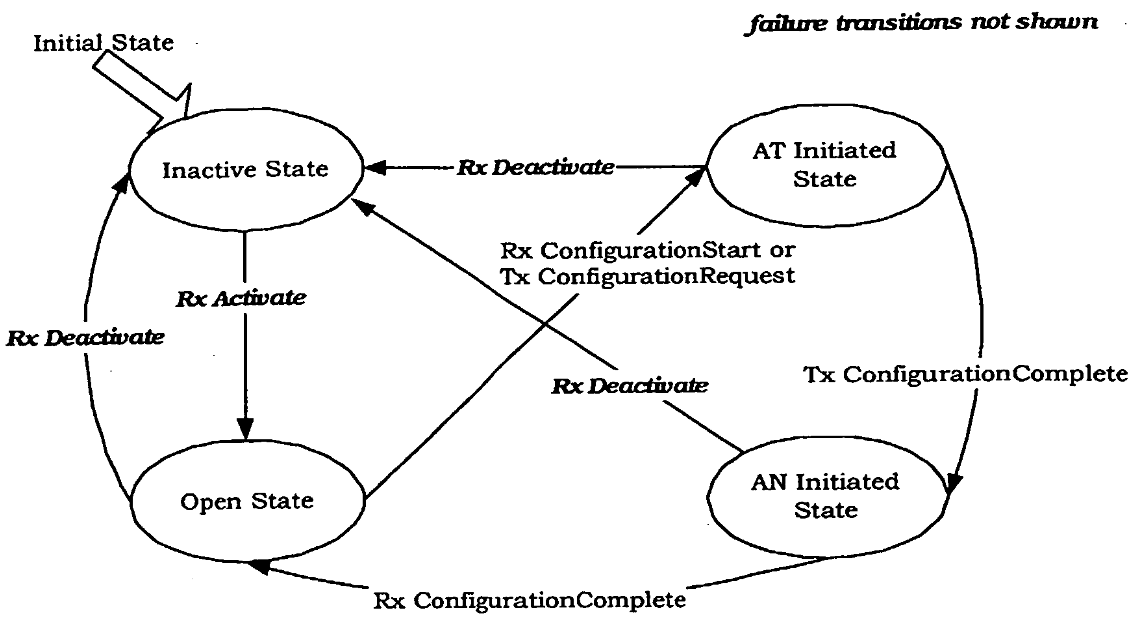


Figure 5.4.1-1. Session Configuration Protocol State Diagram (Access Terminal)

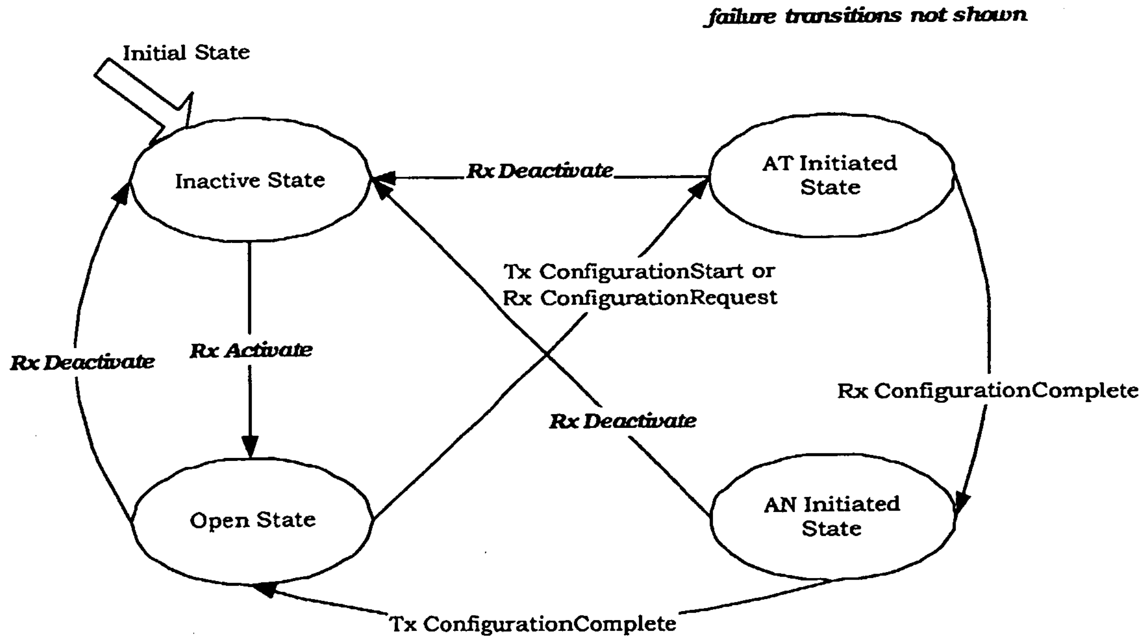


Figure 5.4.1-2. Session Configuration Protocol State Diagram (Access Network)

5.4.2 Primitives and Public Data

5.4.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***

5.4.2.2 Return Indications

This protocol returns the following indications:

- ***SCPChanged***
- ***Reconfigured***
- ***Failed***

5.4.2.3 Public Data

- Type and subtype of all negotiated protocols
- SessionConfigurationToken

5.4.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{SCPType}$.

The Subtype field for this protocol is two octets, set to $N_{SCPDefault}$.

5.4.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

5.4.5 Procedures

5.4.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

This protocol does not have any initial configuration requirements.

5.4.5.2 Processing the Activate Command

If the protocol receives the ***Activate*** command in the Inactive State, it shall transition to the Open State.

If this command is received in any other state it shall be ignored.

5.4.5.3 Processing the Deactivate Command

If the protocol receives the ***Deactivate*** command in the Inactive State it shall be ignored.

If the protocol receives this command in the AT Initiated State, AN Initiated State, or Open State, it shall transition to the Inactive State.

5.4.5.4 Inactive State

Upon entering this state, the protocol shall perform the following:

- Set the SessionConfigurationToken to 0x0000.
- Set the protocols and protocol configurations to their default values.

In this state the protocol waits for the ***Activate*** command. See 5.4.5.2 for processing of the ***Activate*** command in this state.

5.4.5.5 AT Initiated State

During the AT Initiated State of the Default Session Configuration Protocol the access terminal and the access network use the Generic Configuration Protocol (see 10.7) with the access terminal being the initiator of each exchange. The access terminal and the access network use the ConfigurationRequest/ConfigurationResponse exchange defined in 10.7 to select the protocols that will be used for the session.

Also, the access terminal may request restoring a previously established session in this state.

The default values for all the attributes and protocols shall be the values that were agreed upon prior to entering this state.

The protocol in the access terminal or the access network shall return a ***Failed*** indication and transition to the Inactive state, if any of the negotiated protocols declares a failure.

5.4.5.5.1 Access Terminal Requirements

If the access terminal chooses to request restoring a prior session, it shall perform the following in the order specified:

- The access terminal shall construct a 32-bit pseudo random number, Nonce.
- The access terminal shall temporarily configure the protocols within the Security Layer with the parameters (i.e., the session key and all the negotiated protocols and attributes in the security layer) associated with the prior session.
- The access terminal shall supply the Nonce, to the security layer of the prior session as if the Nonce is the payload to be transmitted on the Access Channel. The access terminal shall set all the unspecified parameters needed by the protocols in the Security Layer to zero for the purpose of generating this Security Layer Packet.
- The access terminal shall restore the Security Layer to its previous configuration.
- The access terminal shall set the SecurityPacket variable to the Security Layer Packet constructed in the previous step.

- The access terminal shall send the UATI corresponding to the prior session and the SecurityPacket variables as a complex attribute (see 5.4.6.3.2)a in ConfigurationRequest message.

The access terminal may send the access network ConfigurationRequest messages, requesting the use of specific protocols per the Generic Configuration Protocol.

The access terminal shall process the ConfigurationResponse messages it receives per the Generic Configuration Protocol.

Following the receipt of a ConfigurationResponse message, the access terminal may:

- Send another ConfigurationRequest message attempting to negotiate a different protocol for the protocol Type specified in the ConfigurationResponse message.
- Use the protocol configuration procedures defined by the protocol to perform access terminal-initiated parameter configuration.

If after performing access terminal-initiated parameter configuration, the access terminal requires the use of a different protocol for this protocol Type, the access terminal may send the access network a new ConfigurationRequest message.

If the access terminal sends a ConfigurationRequest message specifying a protocol Type for which protocol negotiation procedures were previously executed in this state, the access terminal shall discard all parameters negotiated during that procedure.

If the protocol in access terminal requires no further negotiation of protocols or configuration of negotiated protocols, it shall send a ConfigurationComplete message to the access network and transition to the AN Initiated State.

5.4.5.5.2 Access Network Requirements

If the access network receives a ConfigurationRequest message from the access terminal, it shall process it and shall respond with a ConfigurationResponse message per the Generic Configuration Protocol.

Once the access network sends a ConfigurationResponse message for a particular protocol, it shall be ready to execute the access terminal-initiated configuration procedures that are particular to that protocol.

If the access network receives a ConfigurationRequest message, specifying a protocol Type for which it has previously executed a parameter negotiation procedure, the access network shall discard all parameters negotiated during that procedure.

If the protocol in the access network receives a ConfigurationComplete message, it shall transition to the AN Initiated State.

5.4.5.6 AN Initiated State

During the AN Initiated State of the protocol, the access network and the access terminal execute the access network-initiated configuration procedures specified by each negotiated protocol. These procedures typically allow the access network to override default values otherwise used by the access terminal.

If the access network initiates negotiation of an attribute, the default value for the attribute shall be the value agreed upon prior to entering this state.

5.4.5.6.1 Access Terminal Requirements

In this protocol state the access terminal shall be ready to execute the access network-initiated configuration procedures particular to each protocol used during the session.

If the access terminal receives a ConfigurationRequest message from the access network, it shall process it and shall respond with a ConfigurationResponse message according to the Generic Configuration Protocol.

If the access terminal receives a ConfigurationComplete message it shall:

- Issue an ***AirlinkManagement.CloseConnection*** command.
- Return a ***Reconfigured*** indication.
- Transition to the Open State.

If as a result of ConfigurationRequest/ConfigurationResponse exchange a non-default Session Configuration Protocol is selected, the access terminal shall return an ***SCPChanged*** indication.

If as a result of ConfigurationRequest/ConfigurationResponse exchange a PriorSession attribute (with a non-zero Restore field) is agreed upon, the protocols and attributes corresponding to the session specified by the PriorSession attribute shall take effect after the protocol receives a ***ConnectedState.ConnectionClosed*** indication. Otherwise, the newly negotiated protocols and attributes shall take effect after the protocol receives ***ConnectedState.ConnectionClosed*** indication.

5.4.5.6.2 Access Network Requirements

In this protocol state, the access network may execute the access network-initiated configuration procedures that are particular to each protocol used during the session.

If the access network chooses to negotiate a different Session Configuration Protocol, it shall initiate the Session Configuration Protocol selection (i.e., sending ConfigurationRequest message specifying protocol Type of $N_{SCPType}$) prior to selection of any other protocol.

The access network may set the SessionConfigurationToken field of the ConfigurationComplete message to reflect the selected protocols and the negotiation parameters associated with the negotiated protocols. The rules for setting this field are outside the scope of this specification.

If the protocol in access network requires no further negotiation of protocols or configuration of negotiated protocols, it shall:

- Send a ConfigurationComplete message to the access terminal.
- Issue an ***AirlinkManagement.CloseConnection*** command.
- Return a ***Reconfigured*** indication.

- Transition to the Open State.

If as a result of ConfigurationRequest/ConfigurationResponse exchange a non-default Session Configuration Protocol is selected, the access network shall return an ***SCPChanged*** indication.

If as a result of ConfigurationRequest/ConfigurationResponse exchange a PriorSession attribute (with a non-zero Restore field) is agreed upon, the protocols and attributes corresponding to the session specified by the PriorSession attribute shall take effect after the protocol receives a ***ConnectedState.ConnectionClosed*** indication. Otherwise, the newly negotiated protocols and attributes shall take effect after the protocol receives ***ConnectedState.ConnectionClosed*** indication.

5.4.5.7 Open State

5.4.5.7.1 General Requirements

In this protocol state the access terminal and the access network use the negotiated protocols to exchange data and signaling in accordance with the requirements of each protocol.

The protocol in the access network may send a ConfigurationStart message at any time during the Open State to start the negotiation process (e.g., the access network may send this message to negotiate a new stream).

The protocol in the access terminal may send a ConfigurationRequest message at any time during the Open State to start the negotiation process (e.g., the access terminal may send this message to negotiate a new stream).

The protocol in the access terminal transitions to the AT Initiated State when it receives a ConfigurationStart message or when it sends a ConfigurationRequest message.

The protocol in the access network transitions to the AT Initiated State when it sends a ConfigurationStart message or when it receives a ConfigurationRequest message.

5.4.6 Message Formats

5.4.6.1 ConfigurationComplete

The sender sends the ConfigurationComplete message to indicate that it has completed the negotiation procedures performed at its initiative.

Field	Length (bits)
MessageID	8
TransactionID	8
SessionConfigurationToken	0 or 16

MessageID The sender shall set this field to 0x00.

TransactionID The access terminal shall increment this value for each new ConfigurationComplete message sent. The access network shall set this value to the value of TransactionID included in the last ConfigurationComplete message received from the access terminal.

SessionConfigurationToken
Session Configuration Token. The access terminal shall omit this field. The access network shall include this field. The access network may set this field to a 16-bit value that reflects the selected protocols and the negotiation parameters associated with the negotiated protocols.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

5.4.6.2 ConfigurationStart

The access network sends this message to start a session configuration process.

Field	Length (bits)
MessageID	8

MessageID The sender shall set this field to 0x01.

Channels	CC FTC	SLP	Best Effort
Addressing	unicast	Priority	40

5.4.6.3 Configuration Messages

The Default Session Configuration Protocol uses the Generic Configuration Protocol for configuration. All configuration messages sent by this protocol shall have their Type field set to $N_{SCPType}$.

The following attribute-value pairs are defined (see 10.3 for attribute record format). All attribute fields for the Default Session Configuration Protocol are two octets in length. .

5.4.6.3.1 Protocol Type Attributes

The Protocol Type configurable attributes are listed in Table 5.4.6.3.1-1. All these attributes are simple. The Attribute ID field for all these attributes are two octets in length and the value fields for these attributes are two octets in length

Table 5.4.6.3.1-1. Protocol Type Configurable Attributes

Attribute ID	Attribute	Values	Meaning
0x00NN	Protocol Type, where NN is the hexadecimal Protocol Type value.	*0x0000*	Default Protocol Subtype.
		0x0000 – 0xFFFF	Protocol Subtype.

5.4.6.3.2 PriorSession Attribute

The following complex attribute and default values are defined (see 10.3 for attribute record definition):

Field	Length (bits)	Default
Length	8	N/A
AttributeID	16	N/A

One or more of the following record:

ValueID	8	N/A
Restore	1	'0'
Reserved	7	'0000000'
UATI	0 or 128	N/A
SecurityPacketLength	0 or 8	N/A
SecurityPacket	0 or SecurityPacketLength × 8	N/A

Length
Length of the complex attribute in octets. The access terminal shall set this field to the length of the complex attribute excluding the Length field.

AttributeID
The access terminal shall set this field to 0x1000.

ValueID
The access terminal shall set this field to an identifier assigned to this complex value.

Restore — The access terminal shall set this field to '1' if it is requesting to restore a prior session. The access terminal shall set this field to '0' if it is requesting to proceed with the current session configuration and not restore any prior sessions.

Reserved — The access terminal shall set this field zero. The access network shall ignore this field.

UATI — The access terminal shall include this field only if the Restore field is set to '1'. If included, the access terminal shall set this field to the UATI associated with the prior session.

SecurityPacketLength

The access terminal shall include this field only if the Restore field is set to '1'. If included, the access terminal shall set this field to the length of the SecurityPacket filed in octets.

SecurityPacket — The access terminal shall include this field only if the Restore field is set to '1'. If included, the access terminal shall set this field to the SecurityPacket variable which is constructed as specified in 5.4.5.5.1.

5.4.6.3.3 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for the Session Configuration Protocol.[6] The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC
Addressing	unicast

SLP	Reliable
Priority	40

5.4.6.3.4 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

[6] Most of the Session Configuration Prot col parameters being configured are the specific (i.e., Subtype) protocols used for each protocol Type.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

5.4.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{SCPType}$	Type field for this protocol	Table 2.3.6-1
$N_{SCPDefault}$	Subtype field for this protocol	0x0000

5.4.8 Interface to Other Protocols

5.4.8.1 Commands

This protocol issues the following command:

- ***AirLinkManagement.CloseConnection***

5.4.8.2 Indications

This protocol registers to receive the following indication:

- ***ConnectedState.ConnectionClosed***

5.4.9 Message Flows

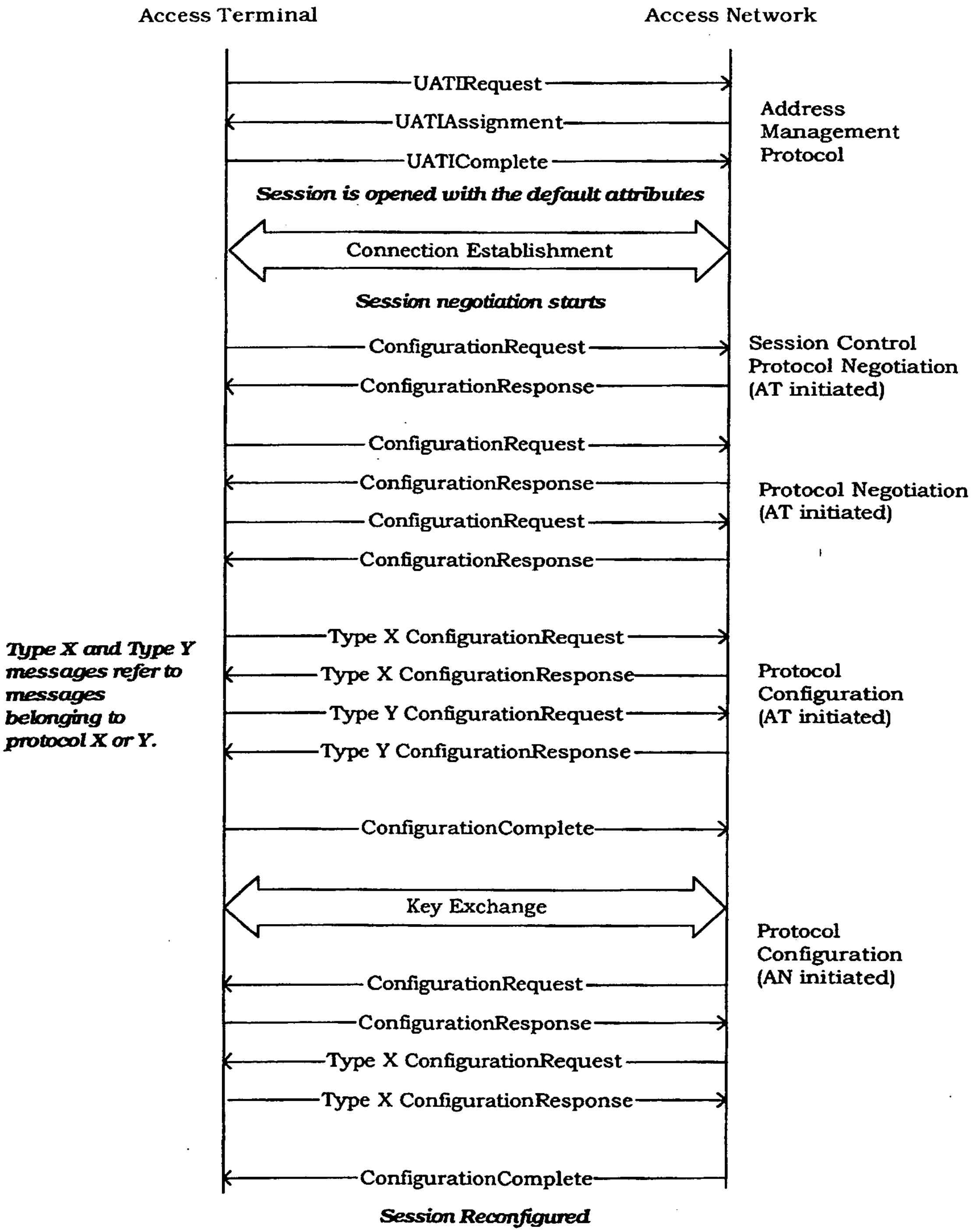

Access Terminal
Access Network
UATIRequest
UATIAssignment
UATIComplete
Address Management Protocol
Session is opened with the default attributes
Connection Establishment
Session negotiation starts
ConfigurationRequest
ConfigurationResponse
Session Control Protocol Negotiation (AT initiated)
ConfigurationRequest
ConfigurationResponse
ConfigurationRequest
ConfigurationResponse
Protocol Negotiation (AT initiated)
Type X and Type Y messages refer to messages belonging to protocol X or Y.
Type X ConfigurationRequest
Type X ConfigurationResponse
Type Y ConfigurationRequest
Type Y ConfigurationResponse
Protocol Configuration (AT initiated)
ConfigurationComplete
Key Exchange
Protocol Configuration (AN initiated)
ConfigurationRequest
ConfigurationResponse
Type X ConfigurationRequest
Type X ConfigurationResponse
ConfigurationComplete
Session Reconfigured

Figure 5.4.9-1. Default Session Configuration Protocol: Extensive Negotiation Procedure

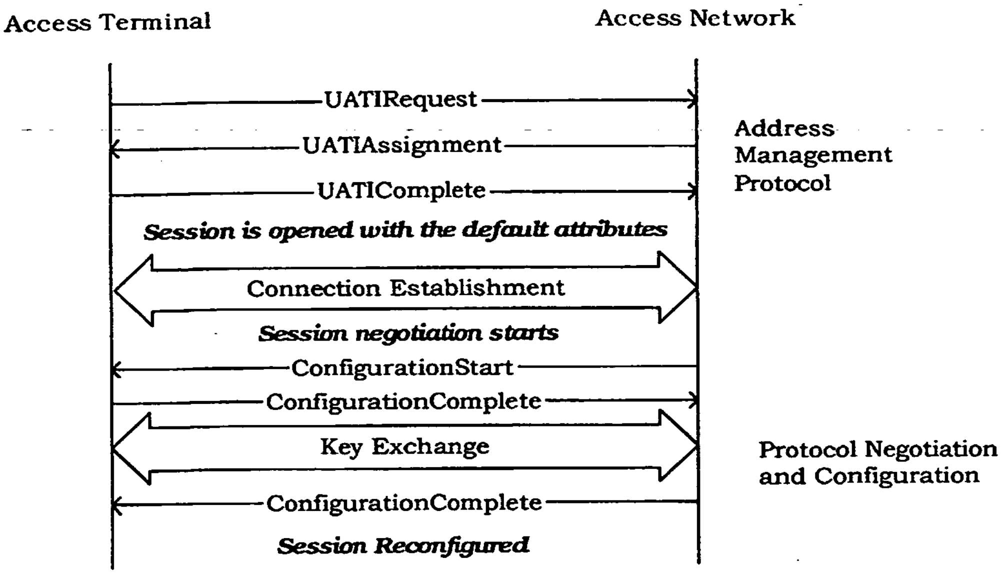


Figure 5.4.9-2. Default Session Configuration Protocol: Minimal Negotiation Procedure with Key Exchange

No text.

6 CONNECTION LAYER

6.1 Introduction

6.1.1 General Overview

The Connection Layer controls the state of the air-link, and it prioritizes the traffic that is sent over it.

This section presents the default protocols for the Connection Layer. With the exception of the Overhead Messages Protocol, each of these protocols can be independently negotiated at the beginning of the session.

The access terminal and the access network maintain a connection whose state dictates the form in which communications between these entities can take place. The connection can be either closed or open:

- Closed Connection: When a connection is closed, the access terminal is not assigned any dedicated air-link resources. Communications between the access terminal and the access network are conducted over the Access Channel and the Control Channel.
- Open Connection: When a connection is open, the access terminal can be assigned the Forward Traffic Channel, and is assigned a Reverse Power Control Channel and a Reverse Traffic Channel. Communications between the access terminal and the access network are conducted over these assigned channels, as well as over the Control Channel.

The Connection Layer provides the following connection-related functions:

- Manages initial acquisition of the network.
- Manages opening and closing of connections.
- Manages communications when connection is closed and when a connection is open.
- Maintains approximate access terminal's location in either connection states.
- Manages radio link between the access terminal and the access network when a connection is open.
- Performs supervision both when the connection is open and when it is closed.
- Prioritizes and encapsulates transmitted data received from the Session Layer and forwards it to the Security Layer.
- De-capsulates data received from the Security Layer and forwards it to the Session Layer.

The Connection Layer performs these functions through the following protocols:

- Air Link Management Protocol: This protocol maintains the overall connection state in the access terminal and the access network. The protocol can be in one of three states, corresponding to whether the access terminal has yet to acquire the network (Initialization State), has acquired the network but the connection is closed (Idle State), or has an open connection with the access network (Connected State). This protocol activates one of the following three protocols as a function of its current state.

- Initialization State Protocol: This protocol performs the actions associated with acquiring an access network.

- Idle State Protocol: This protocol performs the actions associated with an access terminal that has acquired the network, but does not have an open connection. Mainly, these are keeping track of the access terminal's approximate location in support of efficient Paging (using the Route Update Protocol), the procedures leading to the opening of a connection, and support of access terminal power conservation.

- Connected State Protocol: This protocol performs the actions associated with an access terminal that has an open connection. Mainly, these are managing the radio link between the access terminal and the access network (handoffs, handled via the Route Update Protocol), and the procedures leading to the close of the connection.

In addition to the above protocols, which deal with the state of the connection, the Connection Layer also contains the following protocols:

- Route Update Protocol: This protocol performs the actions associated with keeping track of an access terminal's location and maintaining the radio link between the access terminal and the access network. This protocol performs supervision on the pilots.

- Overhead Messages Protocol: This protocol broadcasts essential parameters over the Control Channel. These parameters are shared by protocols in the Connection Layer as well as protocols in other layers. This protocol also performs supervision on the messages necessary to keep the Connection Layer functioning.

- Packet Consolidation Protocol: This protocol consolidates and prioritizes packets for transmission as a function of their assigned priority and the target transmission channel.

Figure 6.1.1-1 illustrates the relationship between all the Connection Layer protocols. An arrow between two protocols implies that the source sends commands to the target.

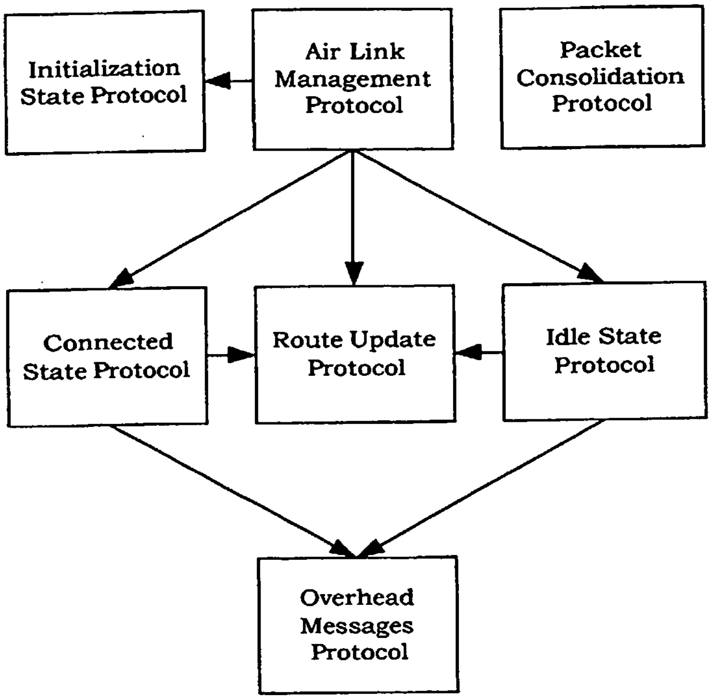

Initialization State Protocol
Air Link Management Protocol
Packet Consolidation Protocol
Connected State Protocol
Route Update Protocol
Idle State Protocol
Overhead Messages Protocol

Figure 6.1.1-1. Connection Layer Protocols

The Air Link Management Protocol, its descendants and the Overhead Messages Protocol are control protocols. The Packet Consolidation Protocol operates on transmitted and received data.

6.1.2 Data Encapsulation

In the transmit direction, the Connection Layer receives Session Layer packets, adds Connection Layer header(s) and padding, where applicable, and forwards the resulting packet for transmission to the Security Layer.

In the receive direction, the Connection Layer receives Security Layer packets from the Security Layer, and forwards them to the Session Layer after taking off the Connection Layer headers and padding.

Figure 6.1.2-1 and Figure 6.1.2-2 illustrate the relationship between Session Layer packets, Connection Layer packets and Security Layer payloads for Format A (maximum size) and Format B Connection Layer packets.

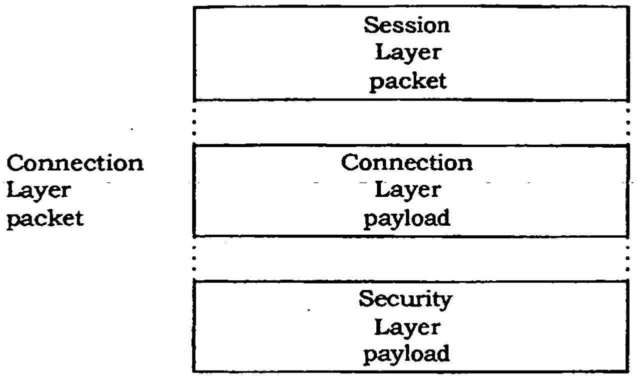


Figure 6.1.2-1. Connection Layer Encapsulation (Format A)

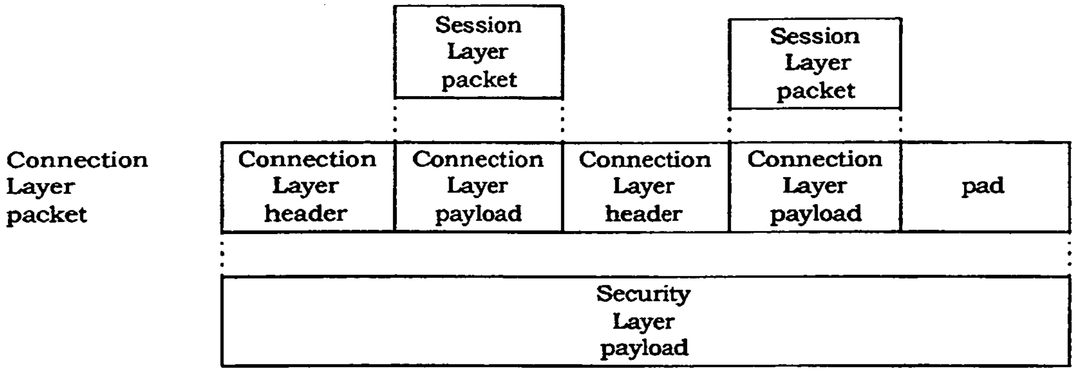


Figure 6.1.2-2. Connection Layer Encapsulation (Format B)

6.2 Default Air-Link Management Protocol

6.2.1 Overview

The Default Air-Link Management Protocol provides the following functions:

- General state machine and state-transition rules to be followed by an access terminal and an access network for the Connection Layer
- Activation and deactivation of Connection Layer protocols applicable to each protocol state
- Mechanism through which access network can redirect access terminal to another network

The actual behavior and message exchange in each state is mainly governed by protocols that are activated by the Default Air-Link Management Protocol. These protocols return indications which trigger the state transitions of this protocol. These protocols also share data with each other in a controlled fashion, by making that data public.

This protocol can be in one of three states:

- Initialization State: In this state the access terminal acquires an access network. The protocol activates the Initialization State Protocol to execute the procedures relevant to this state. The access network maintains a single instance of this state and consequently, executes a single instance of the Initialization State Protocol.
- Idle State: In this state the connection is closed. The protocol activates the Idle State Protocol to execute the procedures relevant to this state.
- Connected State: In this state the connection is open. The protocol activates the Connected State Protocol to execute the procedures relevant to this state.

Figure 6.2.1-1 provides an overview of the access terminal states and state transitions. All transitions are caused by indications returned from protocols activated by the Default Air-Link Management Protocol.

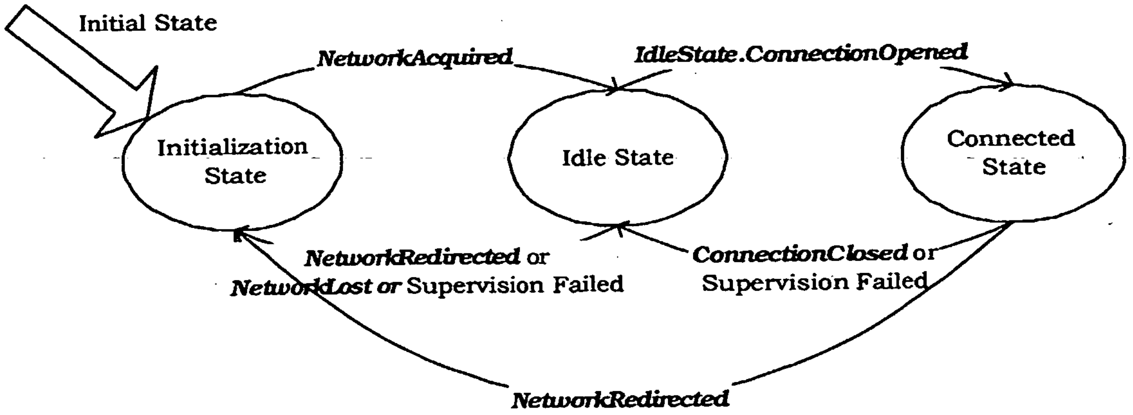

Initial State
NetworkAcquired
IdleState.ConnectionOpened
Initialization State
Idle State
Connected State
NetworkRedirected or NetworkLost or Supervision Failed
ConnectionClosed or Supervision Failed
NetworkRedirected

Figure 6.2.1-1. Air Link Management Protocol State Diagram (Access Terminal)

Figure 6.2.1-2 provides an overview of the access network states and state transitions.

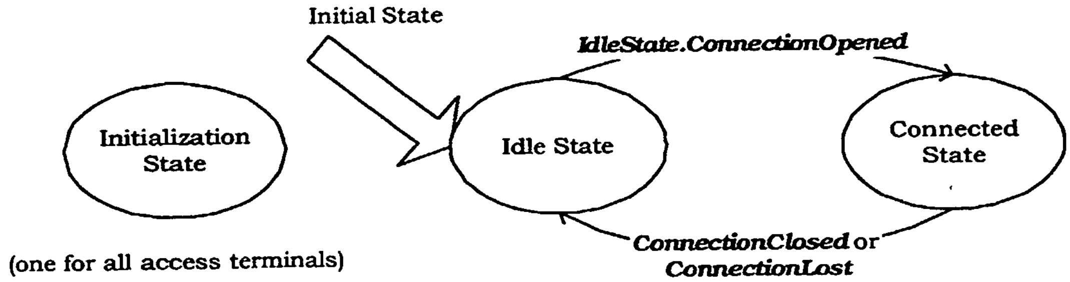

Initial State
IdleState.ConnectionOpened
Initialization State
Idle State
Connected State
(one for all access terminals)
ConnectionClosed or ConnectionLost

Figure 6.2.1-2. Air Link Management Protocol State Diagram (Access Network)

Table 6.2.1-1 provides a summary of the Connection Layer and MAC Layer protocols that are active in each state.

Table 6.2.1-1. Active Protocols Per Air Link Management Protocol State

Initialization State	Idle State	Connected State
Overhead Messages Protocol	Overhead Messages Protocol	Overhead Messages Protocol
Initialization State Protocol	Idle State Protocol	Connected State Protocol
Control Channel MAC Protocol[7]	Route Update Protocol	Route Update Protocol
	Control Channel MAC Protocol	Control Channel MAC Protocol
	Access Channel MAC Protocol	Forward Traffic Channel MAC Protocol
	Forward Traffic Channel MAC Protocol[8]	Reverse Traffic Channel MAC Protocol
	Reverse Traffic Channel MAC Protocol[9]	

6.2.2 Primitives and Public Data

6.2.2.1 Commands

This protocol defines the following commands:

- *OpenConnection*
- *CloseConnection*

6.2.2.2 Return Indications

This protocol does not return any indications.

6.2.2.3 Public Data

- None.

6.2.3 Basic Protocol Numbers

The Type field for the Air-Link Management Protocol is one octet, set to $N_{ALMPType}$.

The Subtype field for the Default Air-Link Management Protocol is two octets, set to $N_{ALMPDefault}$.

[7] Activated by the Initialization State Protocol

[8] Only during connection setup

[9] Only during connection setup

6.2.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

6.2.5 Procedures

6.2.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Initialization State for the access terminal.

This protocol shall have a single instance operating in the Initialization State at the access network, serving all access terminals.

This protocol shall have a single instance for each access terminal with which the access network is currently maintaining a session. This instance shall be started in the Idle State.

This protocol does not have any initial configuration requirements.

6.2.5.2 Command Processing

6.2.5.2.1 OpenConnection

If the protocol receives the ***OpenConnection*** command in the Initialization State, the access terminal shall queue the command and execute it when the access terminal enters the Idle State.

The access network shall ignore the command in the Initialization State.

If the protocol receives this command in the Idle State:

- Access terminal shall issue an ***IdleState.OpenConnection*** command.
- Access network shall issue an ***IdleState.OpenConnection*** command.

If the protocol receives this command in the Connected State the command shall be ignored.

6.2.5.2.2 CloseConnection

If the protocol receives the ***CloseConnection*** command in the Connected State:

- Access terminal shall issue a ***ConnectedState.CloseConnection*** command.
- Access network shall issue a ***ConnectedState.CloseConnection*** command.

If the protocol receives this command in any other state it shall be ignored.

6.2.5.3 Initialization State

In the Initialization State the access terminal has no information about the serving access network. In this state the access terminal selects a serving access network and obtains time synchronization from the access network.

6.2.5.3.1 Access Terminal Requirements

The access terminal shall enter the Initialization State when the Default Air-Link Management Protocol is instantiated. This may happen on events such as network redirection and initial power-on. A comprehensive list of events causing the Default Air-Link Management Protocol to enter the Initialization State is beyond the scope of this specification.

The access terminal shall issue an ***InitializationState.Activate*** command upon entering this state. If the access terminal entered this state because the protocol received a Redirect message and a Channel Record was received with the message, the access terminal shall provide the Channel Record with the command.

If the protocol receives an ***InitializationState.NetworkAcquired*** indication the access terminal shall issue an ***InitializationState.Deactivate*** command[10] and transition to the Idle State.

6.2.5.3.2 Access Network Requirements

The access network shall constantly execute a single instance of the Initialization State Protocol. The access network shall constantly execute a single instance of the Overhead Messages Protocol.

6.2.5.4 Idle State

In this state the access terminal has acquired the access network but does not have an open connection with the access network.

6.2.5.4.1 Access Terminal Requirements

6.2.5.4.1.1 General Requirements

The access terminal shall issue the following commands upon entering this state:

- ***IdleState.Activate***
- ***RouteUpdate.Activate***
- ***AccessChannelMAC.Activate.***

If the access terminal had a queued ***OpenConnection*** command, it shall issue an ***IdleState.OpenConnection*** command.

If the protocol receives an ***IdleState.ConnectionOpened*** indication, the access terminal shall perform the cleanup procedures defined in 6.2.5.4.1.2 and transition to the Connected State.

If the protocol receives a Redirect message, a ***RouteUpdate.NetworkLost***, an ***OverheadMessages.SupervisionFailed***, an ***OverheadMessages.ANRedirected***, a

[10] Some of the ***Deactivate*** commands issued by this protocol are superfluous (because the commanded protocol already put itself in the Inactive State) but are specified here for completeness.

ControlChannelMAC.SupervisionFailed, an ***AccessChannelMAC.SupervisionFailed,*** or an ***AccessChannelMAC.TransmissionFailure*** indication, the access terminal shall:

- Issue a ***RouteUpdate.Deactivate*** command,
- Issue an ***OverheadMessages.Deactivate*** command,
- Issue a ***ControlChannelMAC.Deactivate*** command,
- Perform the cleanup procedures defined in 6.2.5.4.1.2, and
- Transition to the Initialization State.

6.2.5.4.1.2 Idle State Cleanup Procedures

The access terminal shall issue the following commands when it exits this state:

- ***IdleState.Deactivate***
- ***AccessChannelMAC.Deactivate***

6.2.5.4.2 Access Network Requirements

6.2.5.4.2.1 General Requirements

The access network shall issue the following commands upon entering this state:

- ***IdleState.Activate***
- ***RouteUpdate.Activate***

If the protocol receives an ***IdleState.ConnectionOpened*** indication, the access network shall perform the cleanup procedures defined in 6.2.5.4.2.2 and transition to the Connected State.

The access network may send the access terminal a Redirect message to redirect it from the current serving network and optionally, provide it with information directing it to another network. If the access network sends a Redirect message it shall

- Issue a ***RouteUpdate.Deactivate*** command,
- Perform the cleanup procedures defined in 6.2.5.4.2.2.

6.2.5.4.2.2 Idle State Cleanup Procedures

The access network shall issue the following command when it exits this state:

- ***IdleState.Deactivate***

6.2.5.5 Connected State

In the Connected State, the access terminal and the access network have an open connection.

6.2.5.5.1 Access Terminal Requirements

6.2.5.5.1.1 General Requirements

The access terminal shall issue the following command upon entering this state:

- ***ConnectedState.Activate***

If the protocol receives a ***ConnectedState.ConnectionClosed***, an ***OverheadMessages.SupervisionFailed***, a ***ControlChannelMAC.SupervisionFailed***,a ***RouteUpdate.AssignmentRejected***, or a ***ForwardTrafficChannelMAC.SupervisionFailed*** indication, the access terminal shall:

- Issue a ***RouteUpdate.Close*** command,[11]
- Issue a ***ControlChannelMAC.Deactivate*** command,
- Issue an ***OverheadMessages.Deactivate*** command,
- Perform the cleanup procedure defined in 6.2.5.5.1.2,
- Transition to the Idle State.

If the protocol receives a Redirect message or an ***OverheadMessages.ANRedirected*** indication, the access terminal shall:

- Issue a ***RouteUpdate.Close*** command,[12]
- Issue a ***ControlChannelMAC.Deactivate*** command,
- Issue an ***OverheadMessages.Deactivate*** command,
- Perform the cleanup procedure defined in 6.2.5.5.1.2,
- Transition to the Initialization State.

6.2.5.5.1.2 Connected State Cleanup Procedures

The access terminal shall issue the following command when it exits this state:

- ***ConnectedState.Deactivate***

6.2.5.5.2 Access Network Requirements

6.2.5.5.2.1 General Requirements

The access network shall issue the following command upon entering this state:

- ***ConnectedState.Activate***

[11] The Route Update Protocol takes care of closing the Forward Traffic Channel MAC and Reverse Traffic Channel MAC Protocols.

[12] The Route Update Protocol takes care of closing the Forward Traffic Channel MAC and Reverse Traffic Channel MAC Protocols.

If the protocol receives a ***ConnectedState.ConnectionClosed***, or ***RouteUpdate.ConnectionLost*** indication, the access network shall:

- Issue a ***RouteUpdate.Close*** command,
- Perform the cleanup procedures defined in 6.2.5.5.2.2,
- Transition to the Idle State.

The access network may send the access terminal a Redirect message to redirect it from the current serving network and optionally, provide it with information directing it to another network. If the access network sends a Redirect message it shall:

- Issue a ***RouteUpdate.Deactivate*** command,
- Perform the cleanup procedures defined in 6.2.5.5.2.2,
- Transition to the Idle State.

6.2.5.5.2.2 Connected State Cleanup Procedures

The access network shall issue the following command when it exits this state:

- ***ConnectedState.Deactivate***

6.2.6 Message Formats

6.2.6.1 Redirect

The access network sends the Redirect message to redirect the access terminal(s) away from the current network; and, optionally, the access network provides it with information directing it to one of a set of different networks.

Field	Length (bits)
MessageID	8
NumChannel	8

NumChannel instances of the following field

Field	Length (bits)
Channel	24

MessageID The access network shall set this field to 0x00.

NumChannel The access network shall set this field to the numbe r of Channel records it is including in this message.

Channel This field shall be set to the channel that the access terminal should reacquire. The channel shall be specified using the standard Channel Record definition, see 10.1.

Channels	CC	FTC
Addressing	broadcast	unicast

SLP	Best Effort
Priority	40

6.2.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{ALMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{ALMPDefault}$	Subtype field for this protocol	0x0000

6.2.8 Interface to Other Protocols

6.2.8.1 Commands Sent

This protocol issues the following commands:

- ***InitializationState.Activate***
- ***InitializationState.Deactivate***
- ***IdleState.Activate***
- ***IdleState.Deactivate***
- ***IdleState.OpenConnection***
- ***ConnectedState.Activate***
- ***ConnectedState.Deactivate***
- ***ConnectedState.CloseConnection***
- ***RouteUpdate.Activate***
- ***RouteUpdate.Deactivate***
- ***RouteUpdate.Close***
- ***OverheadMessages.Deactivate***
- ***ControlChannelMAC.Deactivate***
- ***AccessChannelMAC.Activate***
- ***AccessChannelMAC.Deactivate***

6.2.8.2 Indications

This protocol registers to receive the following indications:

- ***InitializationState.NetworkAcquired***
- ***IdleState.ConnectionOpened***
- ***ConnectedState.ConnectionClosed***
- ***RouteUpdate.ConnectionLost***

- *RouteUpdate.NetworkLost*
- *RouteUpdate.AssignmentRejected*
- *OverheadMessages.ANRedirected*
- *OverheadMessages.SupervisionFailed*
- *ControlChannelMAC.SupervisionFailed*
- *AccessChannelMAC.SupervisionFailed*
- *ForwardTrafficChannelMAC.SupervisionFailed*

6.3 Default Initialization State Protocol

6.3.1 Overview

The Default Initialization State Protocol provides the procedures and messages required for an access terminal to acquire a serving network.

At the access terminal, this protocol operates in one of the following four states:

- Inactive State: In this state the protocol waits for an ***Activate*** command.
- Network Determination State: In this state the access terminal chooses an access network on which to operate.
- Pilot Acquisition State: In this state the access terminal acquires a Forward Pilot Channel.
- Synchronization State: In this state the access terminal synchronizes to the Control Channel cycle, receives the Sync message, and synchronizes to system time.

Protocol states and events causing transition between states are shown in Figure 6.3.1-1.

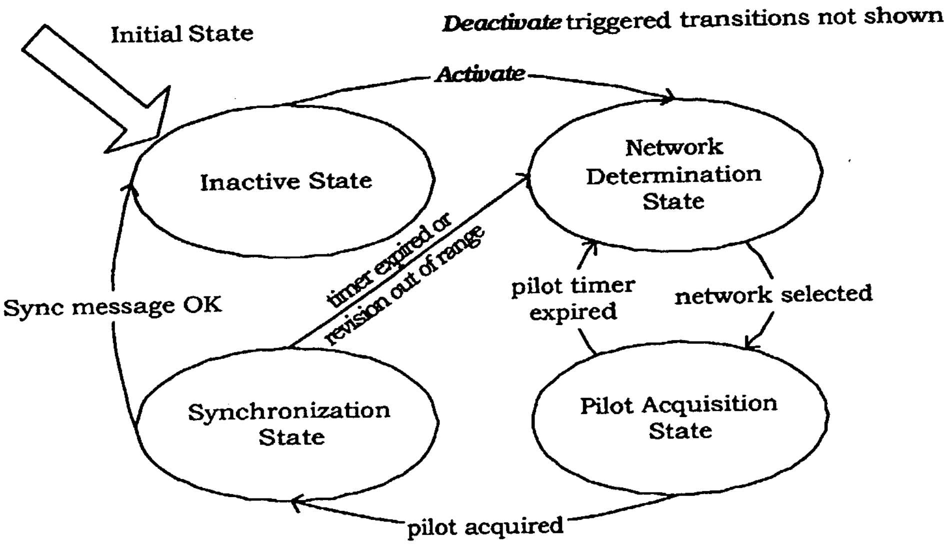


Figure 6.3.1-1. Default Initialization State Protocol State Diagram

6.3.2 Primitives and Public Data

6.3.2.1 Commands

This protocol defines the following commands:

- ***Activate*** (an optional Channel Record can be specified with the command)
- ***Deactivate***

6.3.2.2 Return Indications

This protocol returns the following indications:

- ***NetworkAcquired***

6.3.2.3 Public Data

This protocol makes the following data public:

- Selected channel
- System time
- The following fields of the Sync message:
  - MaximumRevision
  - MinimumRevision
  - PilotPN

6.3.3 Basic Protocol Numbers

The Type field for the Initialization State Protocol is one octet, set to $N_{ISPType}$.

The Subtype field for the Default Initialization State Protocol is two octets, set to $N_{ISPDefault}$.

6.3.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

6.3.5 Procedures

The access network shall broadcast the Sync message periodically in a synchronous Control Channel capsule. This period should not exceed $T_{ISPSync}$ seconds.

The access network need not keep state for this protocol.

6.3.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State for the access terminal.

This protocol does not have any initial configuration requirements.

6.3.5.2 Command Processing

The access network shall ignore all commands.

6.3.5.2.1 Activate

If the protocol receives an ***Activate*** command in the Inactive State, the access terminal shall transition to the Network Determination State.

If the protocol receives this command in any other state, the access terminal shall ignore it.

6.3.5.2.2 Deactivate

If the protocol receives a ***Deactivate*** command in the Inactive State, the access terminal shall ignore it.

If the protocol receives this command in any other state, the access terminal shall transition to the Inactive State.

6.3.5.3 Inactive State

In the Inactive State the access terminal waits for the protocol to receive an ***Activate*** command.

6.3.5.4 Network Determination State

In the Network Determination State the access terminal selects a CDMA Channel (see 10.1) on which to try and acquire the access network.

If a Channel Record was provided with the ***Activate*** command, the access terminal should select the system and channel specified by the record.

The specific mechanisms to provision the access terminal with a list of preferred networks and with the actual algorithm used for network selection are beyond the scope of this specification.

Upon selecting a CDMA Channel the access terminal shall enter the Pilot Acquisition State.

6.3.5.5 Pilot Acquisition State

In the Pilot Acquisition State the access terminal acquires the Forward Pilot Channel of the selected CDMA Channel.

Upon entering the Pilot Acquisition State, the access terminal shall tune to the selected CDMA Channel and shall search for the pilot. If the access terminal acquires the pilot, it shall enter the Synchronization State.[13] If the access terminal fails to acquire the pilot within $T_{ISPPilotAcq}$ seconds of entering the Pilot Acquisition State, it shall enter the Network Determination State.

6.3.5.6 Synchronization State

In the Synchronization State the access terminal completes timing synchronization.

Upon entering this state, the access terminal shall issue the ***ControlChannelMAC.Activate*** command.

[13] The Access Terminal Minimum Performance Requirements contains specifications regarding pilot acquisition performance.

If the access terminal fails to receive a Sync message within $T_{ISPSyncAcq}$ seconds of entering the Synchronization State, the access terminal shall issue a ***ControlChannelMAC.Deactivate*** command and shall enter the Network Determination State. While attempting to receive the Sync message, the access terminal shall discard any other messages received on the Control Channel.

When the access terminal receives a Sync message:

- If the access terminal's revision number is not in the range defined by the MinimumRevision and MaximumRevision fields (inclusive) specified in the message, the access terminal shall issue a ***ControlChannelMAC.Deactivate*** command and enter the Network Determination State.
- Otherwise, the access terminal shall:
  - Set the access terminal time to the time specified in the message; The time specified in the message is the time applicable 160 ms following the beginning of the Control Channel Cycle in which the Sync message was received,
  - Return a ***NetworkAcquired*** indication,
  - Enter the Inactive State.

6.3.6 Message Formats

6.3.6.1 Sync

The access network broadcasts the Sync message to convey basic network and timing information.

Field	Length (bits)
MessageID	2
MaximumRevision	8
MinimumRevision	8
PilotPN	9
SystemTime	37

MessageID The access network shall set this field to '00'.

MaximumRevision Maximum Air-Interface protocol revision supported by the access network. The access network shall set this field to the value specified in 1.14. This value shall be in the range [0x00, 0xff].

MinimumRevision Minimum Air-Interface protocol revision supported by the access network. The access network shall set this field to the value specified in 1.14. This value shall be in the range [0x00, MaximumRevision].

PilotPN Pilot PN Offset. The access network shall set this field to the pilot PN sequence offset for this sector in units of 64 PN Chips.

SystemTime The access network shall set this field to the System Time 160 ms after the start of the Control Channel Cycle in which this Sync message is being sent. The System Time is specified in units of 26.66... ms.

Channels	CCsyn	SLP	Best Effort
Addressing	broadcast	Priority	30

6.3.7 Protocol Numeric Constants

Constant	Meaning	Value	Comments
$N_{ISPType}$	Type field for this protocol	Table 2.3.6-1	
$N_{ISPDefault}$	Subtype field for this protocol	0x0000	
$T_{ISPSync}$	Sync message transmission period	1.28 seconds	3 × Control Channel Cycle
$T_{ISPPilotAcq}$	Time to acquire pilot in access terminal	60 seconds	
$T_{ISPSyncAcq}$	Time to acquire Sync message in access terminal	5 seconds	

6.3.8 Interface to Other Protocols

6.3.8.1 Commands Sent

This protocol issues the following commands:

- *ControlChannelMAC.Activate*
- *ControlChannelMAC.Deactivate*

6.3.8.2 Indications

This protocol does not register to receive any indications.

6.4 Default Idle State Protocol

6.4.1 Overview

The Default Idle State Protocol provides the procedures and messages used by the access terminal and the access network when the access terminal has acquired a network and a connection is not open.

This protocol operates in one of the following four states:

- Inactive State: In this state the protocol waits for an ***Activate*** command.
- Sleep State: In this state the access terminal may shut down part of its subsystems to conserve power. The access terminal does not monitor the Forward Channel, and the access network is not allowed to transmit unicast packets to it.
- Monitor State: In this state the access terminal monitors the Control Channel, listens for Page messages and if necessary, updates the parameters received from the Overhead Messages Protocol. The access network may transmit unicast packets to the access terminal in this state.
- Connection Setup State: In this state the access terminal and the access network set-up a connection.

Protocol states and events causing the transition between the states are shown in Figure 6.4.1-1 and Figure 6.4.1-2.

Deactivate triggered transitions and Fast Connect transitions are not shown

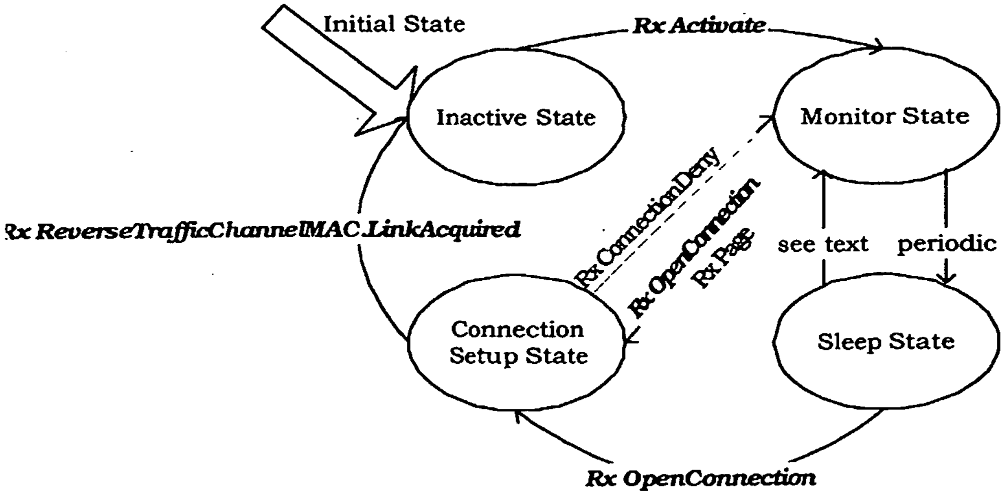


Figure 6.4.1-1. Default Idle State Protocol State Diagram (Access Terminal)

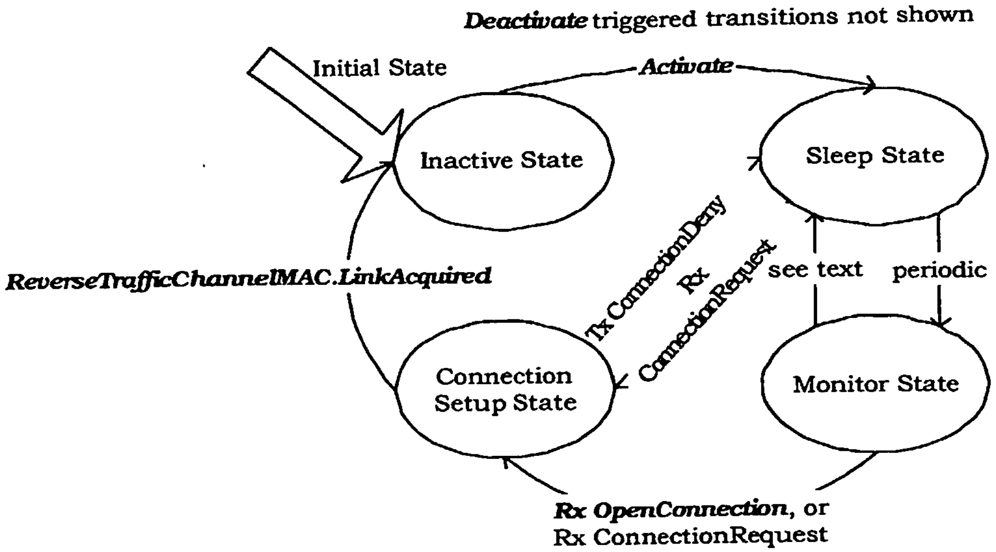


Figure 6.4.1-2. Default Idle State Protocol State Diagram (Access Network)

This protocol supports periodic network monitoring by the access terminal, allowing for significant power savings. The following access terminal operation modes are supported:

- Continuous operation, in which the access terminal continuously monitors the Control Channel.
- Suspended mode operation, in which the access terminal monitors the Control Channel continuously for a period of time and then proceeds to operate in the slotted mode. Suspended mode follows operation in the Air-Link Management Protocol Connected State and allows for quick network-initiated reconnection.
- Slotted mode operation, in which the access terminal monitors only selected slots.

This protocol supports two types of connection set-ups:

- Normal setup: this procedure is always performed at the initiative of the access terminal.[14] It consists of the access terminal sending a ConnectionRequest message which in turn causes the lower layers to open the connection. The Connection Setup State contains the requirements for normal setup.

[14] The access network may transmit a Page message to the access terminal directing it to initiate the procedure.

- Fast Connect: this procedure is always performed at the initiative of the access network and consists of the access network opening the connection directly via a ***RouteUpdate.Open*** command.[15] Fast Connect eliminates the need for the Page / ConnectionRequest exchange when the access network has pending data to transmit to an access terminal, and is especially useful when the access terminal is in suspended mode. Support for Fast Connect at the access network is optional. Support for Fast Connect at the access terminal is mandatory. The Monitor State contains the requirements for Fast Connect.

6.4.2 Primitives and Public Data

6.4.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***
- ***OpenConnection***

6.4.2.2 Return Indications

This protocol returns the following indications:

- ***ConnectionOpened***
- ***ConnectionFailed***

6.4.2.3 Public Data

- None

6.4.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{IDPType}$.

The Subtype field for this protocol is two octets, set to $N_{IDPDefault}$.

6.4.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

[15] This command triggers a transmission of a TrafficChannelAssignment message based on the last RouteUpdate received from the access terminal.

6.4.5 Procedures

6.4.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

This protocol does not have any initial configuration requirements.

6.4.5.2 Command Processing

6.4.5.2.1 Activate

When the protocol receives an ***Activate*** command in the Inactive State:

- The access terminal shall transition to the Monitor State.
- The access network shall transition to the Sleep State.[16]

If the protocol receives this command in any other state it shall be ignored.

6.4.5.2.2 Deactivate

When the protocol receives a ***Deactivate*** command in the Inactive State it shall be ignored.

When the protocol receives this command in any other state:

- The access terminal shall transition to the Inactive State.
- The access network shall transition to the Inactive State.

6.4.5.2.3 OpenConnection

When the protocol receives an ***OpenConnection*** command in the Inactive State or the Connection Setup State, the command shall be ignored.

When the protocol receives this command in the Sleep State:

- The access terminal shall transition to the Connection Setup State.
- The access network shall queue the command and execute it when it is in the Monitor State.

When the protocol receives this command in the Monitor State:

- The access terminal shall transition to the Connection Setup State.
- The access network shall send a Page message to the access terminal and transition to the Connection Setup State.

[16] Since the transitions happen asynchronously, this requirement guarantees that the access network will not transmit unicast packets to the access terminal over the Control Channel when the access terminal is not monitoring the channel.

6.4.5.3 Inactive State

When the protocol is in the Inactive State it waits for an ***Activate*** command.

- The access terminal should not monitor the Control Channel in this state.
- The access network shall not transmit unicast packets to the access terminal in this state.

6.4.5.4 Sleep State

When the access terminal is in the Sleep State it may stop monitoring the Control Channel by issuing the following commands:

- ***OverheadMessages.Deactivate***
- ***ControlChannelMAC.Deactivate***

The access terminal may shut down processing resources to reduce power consumption.

If the access terminal requires opening a connection, it shall transition to the Connection Setup State.

When the access network is in the Sleep State, it is prohibited from sending unicast packets to the access terminal.

If the access network receives a ConnectionRequest message, it shall transition to the Connection Setup State.

The access network and the access terminal shall transition from the Sleep State to the Monitor State in time to send and receive, respectively, the synchronous capsule sent in each Control Channel cycle **C** satisfying

$$(\mathbf{C} + \mathbf{R}) \bmod N_{IDPSleep} = 0$$

where **C** is the number of Control Channel cycles since the beginning of system time and **R** is obtained as follows:

- If PreferredControlChannelCycleEnabled is equal to '0', then **R** is the result of applying the hash function (see 10.4) using the following parameters:
  - Key = SessionSeed
  - Decorrelate = 6 × SessionSeed[11:0]
  - N = $N_{IDPSleep}$
  - where SessionSeed is given as public data of the Address Management Protocol.
- If PreferredControlChannelCycleEnabled is equal to '1', then **R** is set to PreferredControlChannelCycle.

6.4.5.5 Monitor State

When the access terminal is in the Monitor State, it continuously monitors the Control Channel.

When the access network is in the Monitor State, it may send unicast packets to the access terminal.

6.4.5.5.1 Access Terminal Requirements

Upon entering the Monitor State, the access terminal shall issue the following commands:

- *OverheadMessages.Activate*
- *ControlChannelMAC.Activate*

The access terminal shall comply with the following requirements when in the Monitor State:

- Access terminal shall select the CDMA Channel as specified in 6.4.5.5.1.1.
- Access terminal shall monitor the overhead messages as specified in the Overhead Messages Protocol (see 6.8.5.5).
- If the access terminal receives a Page message, it shall transition to the Connection Setup State.
- If the access terminal requires opening a connection, it shall transition to the Connection Setup State.
- If the access terminal receives a *ReverseTrafficChannelMAC.LinkAcquired* indication it shall return a *ConnectionOpened* indication and transition to the Inactive State.[17]
- Access terminal may transition to the Sleep State if the requirements specified in 6.4.5.5.1.2 are satisfied.

6.4.5.5.1.1 CDMA Channel Selection

Each time the content of the SectorParameters message changes, the access terminal shall select a CDMA Channel from the list of channels in the message. If no channels are listed, the access terminal shall use the channel it is currently monitoring. If one or more channels are available, the access terminal shall use the hash function (see 10.4) to compute an index into the channel list provided in the message. The access terminal shall use the following hash function parameters to obtain this index:

- Key = SessionSeed
- Decorrelate = 0
- N = NumChannels field of the SectorParameters message

Where SessionSeed is provided as public data by the AddressManagement Protocol.

6.4.5.5.1.2 Transition to Sleep State

The access terminal may transition to the Sleep State if all of the following requirements are met:

[17] This requirement provides Fast Connect on the access terminal side.

- Access terminal has received at least one Control Channel synchronous capsule and has determined that the QuickConfig message and SectorParameters message are up to date (see 6.8.5.5).
- Access terminal received an ***AccessChannelMAC.TxEnded*** indication for every ***AccessChannelMAC.TxStarted*** indication it received since entering the Monitor State.[18]
- Access terminal has not advertised a suspend period that is current (see 6.5.5.3.1.1). The suspend period is current if the time advertised in the associated ConnectionClose message is greater than the current system time.[19]

6.4.5.5.2 Access Network Requirements

6.4.5.5.2.1 General Requirements

- Access network shall select the CDMA Channel following the same specifications as the access terminal, see 6.4.5.5.1.1.
- If the access network requires opening a connection with the access terminal, it shall send it a Page message over the Control Channel.
- If the access network receives a ConnectionRequest message, it shall transition to the Connection Setup State.
- Access network may use an accelerated procedure to set-up a connection with the access terminal by bypassing the paging process. The access network should only use this procedure if it has a reasonable estimate of the access terminal's current location. To set-up a connection in an accelerated fashion (Fast Connect) the access network shall:
  - Issue a ***RouteUpdate.Open*** command.
  - Return a ***ConnectionOpened*** indication and transition to the Inactive State, if the protocol receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication.
- Access network shall transition to the Sleep State if the access terminal did not advertise a suspend period that is current.

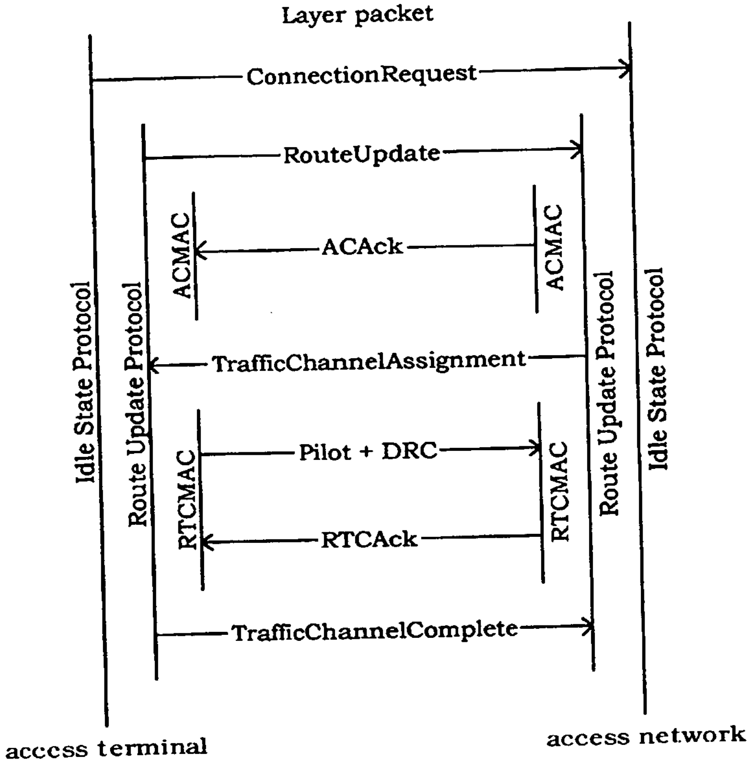
6.4.5.6 Connection Setup State

The access terminal and the access network use the Connection Setup State to perform a normal connection set-up.

[18] This pairing ensures that the access terminal does not have any outstanding messages waiting for an answer.

[19] The access terminal m nitors the Control Channel c ntinuously during a suspend period thus avoiding the delay in opening access network initiated connections due to the sleep period.

Figure 6.4.5.6-1 illustrates the process of opening a connection between the access terminal and the access network when this protocol is used along with the default Route Update and the default Reverse Traffic Channel MAC protocols.[20]



the ConnectionRequest and the RouteUpdate are bundled in the same Access Channel MAC Layer packet

Figure 6.4.5.6-1. Connection Setup Exchange

6.4.5.6.1 Access Terminal Requirements

The access terminal shall comply with the following requirements.

- Upon entering the Connection Setup State the access terminal shall:
    - Issue an ***OverheadMessages.Activate*** command,
    - Issue a ***ControlChannelMAC.Activate*** command,
    -
    - Send a ConnectionRequest message to the access network,
    - Set a state timer for IDPATSetup seconds and start it after receiving an ***AccessChannelMAC.TxEnded*** indication,

[20] The Fast Connect message exchange is identical except for not having the Idle State Protocol ConnectionRequest message and the Route Update Protocol R uteUpdate message.

- If the state timer expires, or if the access terminal receives a ConnectionDeny message, the access terminal shall issue a ***RouteUpdate.Close*** command, return a ***ConnectionFailed*** indication, and transition to the Monitor State,
- If the access terminal receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication, it shall return a ***ConnectionOpened*** indication and transition to the Inactive State.

6.4.5.6.2 Access Network Requirements

If the access network denies the connection request, it should send the access terminal a ConnectionDeny message, shall return a ***ConnectionFailed*** indication, and shall transition to the Sleep State.

Otherwise, the access network shall perform the following:

- Set state timer for $T_{IDPANSetup}$ seconds.
- Issue a ***RouteUpdate.Open*** command.
- If the protocol receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication, the access network shall return a ***ConnectionOpened*** indication and transition to the Inactive State.
- If the state timer expires, the access network shall issue a ***RouteUpdate.Close*** command, return a ***ConnectionFailed*** indication, and transition to the Monitor State.

6.4.6 Message Formats

6.4.6.1 Page

The access network sends the Page message to direct the access terminal to request a connection.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x00.

Channels	CC	SLP	Best Effort
Addressing	unicast	Priority	20

6.4.6.2 ConnectionRequest

The access terminal sends the ConnectionRequest message to request a connection.

Field	Length (bits)
MessageID	8
TransactionID	8
RequestReason	4
Reserved	4

MessageID The access terminal shall set this field to 0x01.

TransactionID The access terminal shall increment this value for each new ConnectionRequest message sent.

RequestReason The access terminal shall set this field to one of the request reasons as shown in Table 6.4.6.2-1.

Table 6.4.6.2-1. Encoding of the RequestReason Field

Field value	Description
0x0	Access Terminal Initiated
0x1	Access Network Initiated
All other values are invalid	

Reserved The access terminal shall set this field to zero. The access network shall ignore this field.

Channels	AC
Addressing	unicast

SLP	Best Effort
Priority	40

6.4.6.3 ConnectionDeny

The access network sends the ConnectionDeny message to deny a connection.

Field	Length (bits)
MessageID	8
TransactionID	8
DenyReason	4
Reserved	4

MessageID The access network shall set this field to 0x02.

TransactionID The access network shall set this value to the TransactionID field of the corresponding ConnectionRequest message.

DenyReason The access network shall set this field to indicate the reason it is denying the connection, as shown in Table 6.4.6.3-1.

Table 6.4.6.3-1. Encoding of the DenyReason Field

Field value	Description
0x0	General
0x1	Network Busy
0x2	Authentication or billing failure
All other values are reserved	

Reserved The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC
Addressing	unicast

SLP	Best Effort
Priority	40

6.4.6.4 Configuration Messages

The Default Idle State Protocol uses the Generic Configuration Protocol for configuration. All configuration messages sent by this protocol shall have their Type field set to $N_{IDPType}$.

The following complex attribute and default values are defined (see 10.3 for attribute record definition):

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PreferredControlChannelCycleEnabled	1	'0'
PreferredControlChannelCycle	0 or 15	N/A
Reserved	7 or 0	N/A

Length Length of the complex attribute in octets. The sender shall set this field to the length of the complex attribute excluding the Length field.

AttributeID The sender shall set this field to 0x00.

ValueID The sender shall set this field to an identifier assigned to this complex value.

PreferredControlChannelCycleEnabled
The sender shall set this field to '1' if PreferredControlChannelCycle field is included in this attribute; otherwise, the sender shall set this field to '0'.

PreferredControlChannelCycle
If PreferredControlChannelCycleEnabled is set to '1', the sender shall include this field and set it to specify the Control Channel Cycle in which the access terminal transitions out of the Sleep State (see 6.4.5.4) in order to monitor the Control Channel. The sender shall omit this field if PreferredControlChannelCycleEnabled is set to '0'.

Reserved The length of this field shall be such that the entire complex attribute is octet-aligned. The sender shall set this field to zero. The receiver shall ignore this field.

6.4.6.4.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for this protocol. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

6.4.6.4.2 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

6.4.7 Protocol Numeric Constants

Constant	Meaning	Value	Comments
$N_{IDPType}$	Type field for this protocol	Table 2.3.6-1	
$N_{IDPDefault}$	Subtype field for this protocol	0x0000	
$N_{IDPSleep}$	Number of control channel cycles constituting a sleep period	0x0c	5.12 seconds
$T_{IDPATSetup}$	Maximum access terminal time in the Connection Setup State	1.5 seconds	
$T_{IDPANSetup}$	Maximum access network time in the Connection Setup State	1 second	

6.4.8 Interface to Other Protocols

6.4.8.1 Commands Sent

This protocol issues the following commands:

- ***RouteUpdate.Open*** (access network only)
- ***RouteUpdate.Close***
- ***OverheadMessages.Activate***
- ***OverheadMessages.Deactivate***
- ***ControlChannelMAC.Activate***
- ***ControlChannelMAC.Deactivate***

6.4.8.2 Indications

This protocol registers to receive the following indications:

- ***ReverseTrafficChannelMAC.LinkAcquired***
- ***AccessChannelMAC.TxStarted***
- ***AccessChannelMAC.TxEnded***

6.5 Default Connected State Protocol

6.5.1 Overview

The Default Connected State Protocol provides procedures and messages used by the access terminal and the access network while a connection is open.

This protocol can be in one of three states:

- Inactive State: In this state the protocol waits for an ***Activate*** command.
- Open State: In this state the access terminal can use the Reverse Traffic Channel and the access network can use the Forward Traffic Channel and Control Channel to send application traffic to each other.
- Close State: This state is associated only with the access network. In this state the access network waits for connection resources to be safely released.

Figure 6.5.1-1 and Figure 6.5.1-2 show the state transition diagrams at the access terminal and the access network respectively.

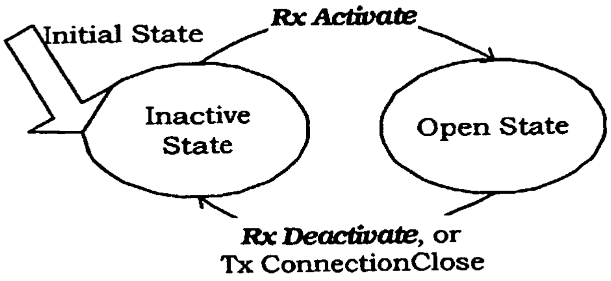


Figure 6.5.1-1. Default Connected State Protocol State Diagram (Access Terminal)

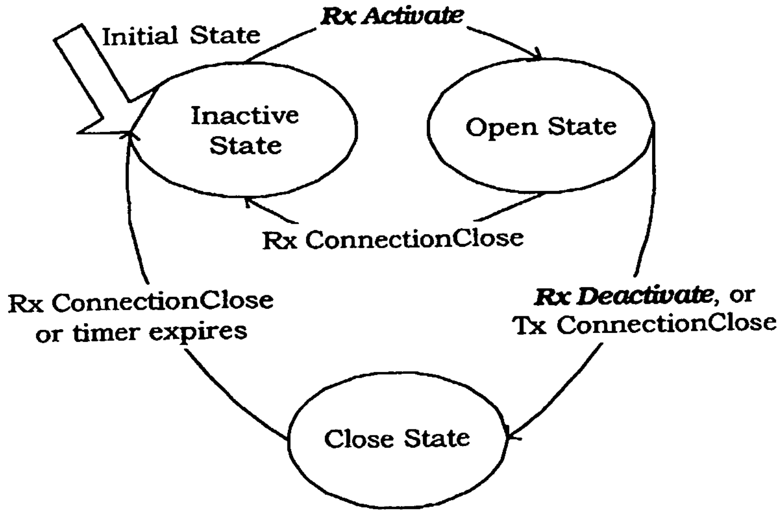


Figure 6.5.1-2. Default Connected State Protocol State Diagram (Access Network)

6.5.2 Primitives and Public Data

6.5.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***
- ***CloseConnection***[21]

6.5.2.2 Return Indications

This protocol returns the following indications:

- ***ConnectionClosed***

6.5.2.3 Public Data

- None

6.5.3 Basic Protocol Numbers

The Type field for the Connected State Protocol is one octet, set to $N_{CSPType}$.

The Subtype field for the Default Connected State Protocol is two octets, set to $N_{CSPDefault}$.

6.5.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

6.5.5 Procedures

6.5.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

This protocol does not have any initial configuration requirements.

6.5.5.2 Command Processing

6.5.5.2.1 Activate

When the protocol receives an ***Activate*** command in the Inactive State:

- The access terminal shall transition to the Open State.
- The access network shall transition to the Open State.

[21] The ***CloseConnection*** command performs the same function as the ***Deactivate*** command and is provided for clarity in the specification.

When the protocol receives this command in any other state it shall be ignored.

6.5.5.2.2 Deactivate

When the protocol receives a ***Deactivate*** command in the Inactive State or in the Close State it shall be ignored.

When the protocol receives this command in the Open State:

- Access terminal shall send a ConnectionClose message to the access network and perform the cleanup procedures defined in 6.5.5.3.1.2.
- Access network shall send a ConnectionClose message to the access terminal, perform the cleanup procedures defined in 6.5.5.3.2.2, and transition to the Close State.

6.5.5.2.3 CloseConnection

The access terminal and the access network shall process the ***CloseConnection*** command following the same procedures used for the ***Deactivate*** command, see 6.5.5.2.2.

6.5.5.3 Open State

In the Open State, the access terminal and the access network maintain a connection and can use it to exchange application traffic on the Reverse Traffic Channel, Forward Traffic Channel, and Control Channel.

6.5.5.3.1 Access Terminal Requirements

6.5.5.3.1.1 General Requirements

Upon entering the Open State, the access terminal shall issue the following commands:

- ***OverheadMessages.Activate***
- ***ControlChannelMAC.Activate***

The access terminal shall comply with the following requirements when in the Open State:

- The access terminal shall receive the Control Channel and the Forward Traffic Channel.
- The access terminal shall not transmit on the Access Channel.
- The access terminal shall monitor the overhead messages as specified in the Overhead Messages Protocol (see 6.8.5.5).
- If the access terminal receives a ConnectionClose message, it shall send ConnectionClose message with CloseReason set to "Close Reply" and execute the cleanup procedures defined in 6.5.5.3.1.2.

If the access terminal sends a ConnectionClose message, it may advertise, as part of the ConnectionClose message, that it shall be monitoring the Control Channel continuously, until a certain time following the closure of the connection. This period is called a suspend period, and can be used by the access network to accelerate the process of sending a unicast packet (and specifically, a Page message or TrafficChannelAssignment message) to the access terminal.

6.5.5.3.1.2 Cleanup Procedures

If the access terminal executes cleanup procedures it shall:

- Issue ***RouteUpdate.Close*** command.
- Return a ***ConnectionClosed*** indication.
- Transition to the Inactive State.

6.5.5.3.2 Access Network Requirements

6.5.5.3.2.1 General Requirements

The access network shall comply with the following requirements when in the Open State:

- Access network shall receive the Reverse Traffic Channel and may transmit on the Forward Traffic Channel.
- If access network receives a ConnectionClose message, it shall consider the connection closed, and it should execute the cleanup procedures defined in 6.5.5.3.2.2 and transition to the Inactive State.
- If access network requires closing the connection, it shall transmit ConnectionClose message, execute the cleanup procedures defined in 6.5.5.3.2.2, and transition to the Close State.

6.5.5.3.2.2 Cleanup Procedures

When the access network performs cleanup procedures it shall:

- Issue ***RouteUpdate.Close*** command,
- Return a ***ConnectionClosed*** indication.

6.5.5.4 Close State

The Close State is associated only with the access network. In this state the access network waits for a replying ConnectionClose message from the access terminal or for an expiration of a timer.

Upon entering this state, the access network shall set a timer for $T_{CSPClose}$ seconds. If the access network receives a ConnectionClose message in this state, or if the timer expires, it may close all connection-related resources assigned to the access terminal, and should transition to the Inactive State.

6.5.6 Message Formats

6.5.6.1 ConnectionClose

The access terminal and the access network send the ConnectionClose message to close the connection.

Field	Length (bits)
MessageID	8
CloseReason	3
SuspendEnable	1
SuspendTime	0 or 36
Reserved	variable

MessageID The sender shall set this field to 0x00.

CloseReason The sender shall set this field to reflect the close reason, as shown in Table 6.5.6.1-1.

Table 6.5.6.1-1. Encoding of the CloseReason Field

Field value	Description
'000'	Normal Close
'001'	Close Reply
'010'	Connection Error
All other values are reserved	

SuspendEnable The access terminal shall set this field to '1' if it will enable a suspend period following the close of the connection. The access network shall set this field to '0'.

SuspendTime Suspend period end time. This field is included only if the SuspendEnable field is set to '1'. The access terminal shall set this field to the absolute system time of the end of its suspend period in units of 80 ms.

Reserved The length of this field shall be such that the entire message is octet-aligned. The sender shall set this field to zero. The receiver shall ignore this field.

Channels	CC FTC RTC
Addressing	unicast

SLP	Best Effort
Priority	40

6.5.7 Protocol Numeric Constants

Constant	Meaning	Value	Comments
$N_{CSPType}$	Type field for this protocol	Table 2.3.6-1	
$N_{CSPDefault}$	Subtype field for this protocol	0x0000	
$T_{CSPClose}$	Access network timer waiting for a responding ConnectionClose message	1.5 seconds	

6.5.8 Interface to Other Protocols

6.5.8.1 Commands Sent

This protocol sends the following commands:

- *RouteUpdate.Close*
- *OverheadMessages.Activate*
- *ControlChannelMAC.Activate*

6.5.8.2 Indications

This protocol does not register to receive any indications.

6.6 Default Route Update Protocol

6.6.1 Overview

The Default Route Update Protocol provides the procedures and messages used by the access terminal and the access network to keep track of the access terminal's approximate location and to maintain the radio link as the access terminal moves between the coverage areas of different sectors.

This protocol can be in one of three states:

- Inactive State: In this state the protocol waits for an ***Activate*** command.
- Idle State: This state corresponds to the Air-Link Management Protocol Idle State. In this state, the access terminal autonomously maintains the Active Set. Route update messages from the access terminal to the access network are based on the distance between the access terminal's current serving sector and the serving sector at the time the access terminal last sent an update.
- Connected State: This state corresponds to the Air-Link Management Protocol Connected State. In this state the access network dictates the access terminal's Active Set. Route update messages from the access terminal to the access network are based on changing radio link conditions.

Transitions between states are driven by commands received from Connection Layer protocols and the transmission and reception of the TrafficChannelAssignment message.

The protocol states, messages and commands causing the transition between the states are shown in Figure 6.6.1-1.

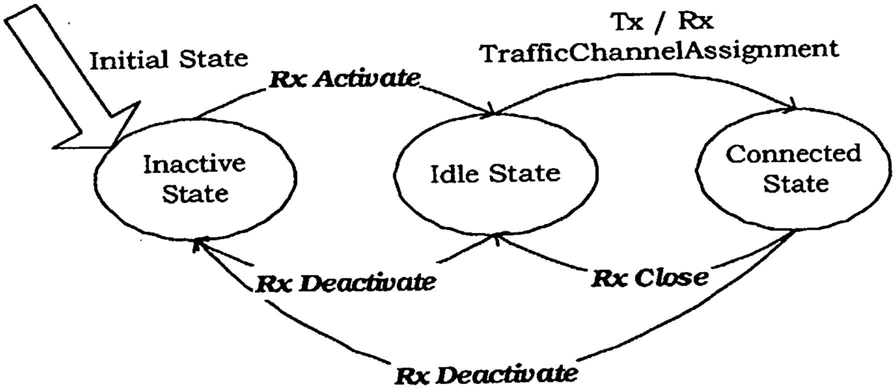


Figure 6.6.1-1. Default Route Update Protocol State Diagram

6.6.2 Primitives and Public Data

6.6.2.1 Commands

This protocol defines the following commands:

- *Activate*
- *Deactivate*
- *Open*
- *Close*

6.6.2.2 Return Indications

This protocol returns the following indications:

- *ConnectionLost* (access network only)
- *NetworkLost*
- *IdleHO*
- *ActiveSetUpdated*
- *RouteUpdate.AssignmentRejected*

6.6.2.3 Public Data

This protocol shall make the following data public:

- Active Set
- Pilot PN for every pilot in the Active Set
- SofterHandoff for every pilot in the Active Set
- MACIndex for every pilot in the Active Set
- Channel record
- FrameOffset
- Current RouteUpdate message

6.6.3 Basic Protocol Numbers

The Type field for the Route Update Protocol is one octet, set to $N_{RUPType}$.

The Subtype field for the Default Route Update Protocol is two octets, set to $N_{RUPDefault}$.

6.6.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocols; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

6.6.5 Procedures

6.6.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

The access network may transmit a ConfigurationRequest message as part of the initial protocol configuration.

The access terminal shall be ready to receive a ConfigurationRequest message during initial protocol configuration.

This protocol shall use the Generic Configuration Protocol to process the ConfigurationRequest and ConfigurationResponse messages (see 10.7).

This protocol uses parameters that are provided, as public data by the Overhead Messages Protocol, or through ConfigurationRequest/ConfigurationResponse message exchanges, or by using a protocol constant. ConfigurationRequest and ConfigurationResponse messages can be sent initially as part of the session negotiation and in the Idle State and the Connected State.

Table 6.6.5.1-1 lists all of the protocol parameters obtained from the public data of the Overhead Messages Protocol. Section 6.6.6.5.1 lists the parameters that can be provisioned through a ConfigurationRequest message, along with the default values the access terminal shall use if it does not receive a ConfigurationRequest message. Section 6.6.7 lists the protocol constants.

Table 6.6.5.1-1. Route Update Protocol Parameters that are Public Data of the Overhead Messages Protocol

RU Parameter	Comment
Latitude	Latitude of sector in units of 0.25 second
Longitude	Longitude of sector in units of 0.25 second
RouteUpdateRadius	Distance between the serving sector and the sector in which location was last reported which triggers a new report. If this field is set to zero, then distance triggered reporting is disabled
NumNeighbors	Number of neighbors specified in the message
NeighborPN	PN Offset of each neighbor in units of 64 PN chips
NeighborChannelIncluded	Set to '1' if a Channel Record is included for the neighbor
NeighborChannel	Neighbor Channel Record specifying network type and frequency

6.6.5.2 Command Processing

6.6.5.2.1 Activate

If the protocol receives an ***Activate*** command in the Inactive State, the access terminal and the access network shall transition to the Idle State.

If this command is received in any other state, it shall be ignored.

6.6.5.2.2 Deactivate

If the protocol receives a ***Deactivate*** command in the Inactive State, it shall be ignored.

If the protocol receives this command in any other state, the access terminal and the access network shall:

- Issue a ***ReverseTrafficChannelMAC.Deactivate*** command,
- Issue a ***ForwardTrafficChannelMAC.Deactivate*** command,
- Transition to the Inactive State.

6.6.5.2.3 Open

If the protocol receives an ***Open*** command in the Idle State,

- The access terminal shall ignore it.
- The access network shall:
  - Transmit a TrafficChannelAssignment message; the access network should base this message on the last RouteUpdate it received from the access terminal,
  - Issue a ***ReverseTrafficChannelMAC.Activate*** command,
  - Issue a ***ForwardTrafficChannelMAC.Activate*** command.
  - Transition to the Connected State.

If this command is received in any other state it shall be ignored.

6.6.5.2.4 Close

If the protocol receives a ***Close*** command in the Connected State the access terminal and the access network shall:

- Issue a ***ReverseTrafficChannelMAC.Deactivate*** command,
- Issue a ***ForwardTrafficChannelMAC.Deactivate*** command,
- Transition to the Idle State.

If this command is received in any other state it shall be ignored.

6.6.5.3 Pilots and Pilot Sets

The access terminal estimates the strength of the Forward Channel transmitted by each sector in its neighborhood. This estimate is based on measuring the strength of the Forward Pilot Channel (specified by the pilot's PN offset and the pilot's CDMA Channel), henceforth referred to as the pilot.

When this protocol is in the Connected State, the access terminal uses pilot strengths to decide when to generate RouteUpdate messages.

When this protocol is in the Idle State, the access terminal uses pilot strengths to decide which sector's Control Channel it monitors.

The following pilot sets are defined to support the Route Update process:[22]

- Active Set: The set of pilots (specified by the pilot's PN offset and the pilot's CDMA Channel) associated with the sectors currently serving the access terminal. When a connection is open, a sector is considered to be serving an access terminal when there is a Forward Traffic Channel, Reverse Traffic Channel and Reverse Power Control Channel assigned to the access terminal. When a connection is not open, a sector is considered to be serving the access terminal when the access terminal is monitoring that sector's control channel.
- Candidate Set: The pilots (specified by the pilot's PN offset and the pilot's CDMA Channel) that are not in the Active Set, but are received by the access terminal with sufficient strength to indicate that the sectors transmitting them are good candidates for inclusion in the Active Set.
- Neighbor Set: The set of pilots (specified by the pilot's PN offset and the pilot's CDMA Channel) that are not in either one of the two previous sets, but are likely candidates for inclusion in the Active Set.
- Remaining Set: The set of all possible pilots (specified by the pilot's PN offset and the pilot's CDMA Channel) on the current channel assignment, excluding the pilots that are in any of the three previous sets.

At any given instant a pilot in the current CDMA Channel is a member of exactly one set.

The access terminal maintains all four sets. The access network maintains only the Active Set.

The access terminal complies with the following rules when searching for pilots, estimating the strength of a given pilot, and moving pilots between sets.

6.6.5.3.1 Neighbor Set Search Window Parameters Update

The access terminal shall maintain RouteUpdateNeighborList which is a list of structures of type Neighbor (defined below). For each pilot (specified by the pilot's PN offset and the pilot's CDMA Channel) in the Neighbor Set, the access terminal shall maintain structure in the RouteUpdateNeighborList.

A Neighbor structure consist of four fields: PilotPN, Channel, SearchWindowSize, and SearchWindowOffset.

The RouteUpdateNeighborList is used by the access terminal to perform pilot search on a pilot in the Neighbor Set.

When this set of procedures are invoked, the access terminal shall perform the following steps in the order specified:

[22] In this context, a pilot identifies a sector.

- For each pilot (specified by its pilot PN and its channel) in the Neighbor Set, the access terminal shall first initialize the corresponding Neighbor structure in RouteUpdateNeighborList as follows:
  - Set the structure's PilotPN field to the neighbor pilot's PN.
  - Set the structure's Channel field to the neighbor pilot's channel record.
  - Set the structure's SearchWindowSize field to the configurable attribute SearchWindowNeighbor.
  - Set the structure's SearchWindowOffset to zero.
- For each pilot (specified by the pilot's PN offset and the pilot's CDMA Channel) listed in the OverheadMessagesNeighborList, the access terminal shall set the non-NULL fields of the corresponding Neighbor structure in the RouteUpdateNeighborList to the fields of the Neighbor structure in the OverheadMessagesNeighborList for this pilot.
- For each pilot (specified by the pilot's PN offset and the pilot's CDMA Channel) listed in the NeighborListMessageNeighborList, the access terminal shall set the non-NULL fields of the corresponding Neighbor structure in the RouteUpdateNeighborList to the fields of the Neighbor structure in the NeighborListMessageNeighborList for this pilot.

6.6.5.3.2 Pilot Search

The access terminal shall continually search for pilots in the Connected State and whenever it is monitoring the Control Channel in the Idle State. The access terminal shall search for pilots in all pilot sets. This search shall be governed by the following rules:

1. Search Priority: The access terminal should use the same search priority for pilots in the Active Set and Candidate Set. In descending order of search rate, the access terminal shall search, most often, the pilots in the Active Set and Candidate Set, then shall search the pilots in the Neighbor Set, and lastly shall search the pilots in the Remaining Set.
2. Search Window Size: The access terminal shall use the search window size specified by the configurable attribute SearchWindowActive for pilots in the Active Set and Candidate Set. For each pilot in the Neighbor Set, the access terminal shall use the search window size specified by Table 6.6.6.5-1 and SearchWindowSize field of the corresponding Neighbor structure in the RouteUpdateNeighborList. The access terminal shall use search window size specified by configurable attribute SearchWindowRemaining for pilots in the Remaining Set.

3. Search Window Center: The access terminal should center the search window around the earliest usable multipath component for pilots in the Active Set. The access terminal should center the search window for each pilot in the Neighbor Set around the pilot's PN sequence offset plus the search window offset specified by Table 6.6.6.5-2 and SearchWindowOffset field of the corresponding Neighbor structure in the RouteUpdateNeighborList using timing defined by the access terminal's time reference (see 9.2.1.5). The access terminal should center the search window around the pilot's PN sequence offset using timing defined by the access terminal's time reference (see 9.2.1.5) for the Remaining Set.

6.6.5.3.3 Pilot Strength Measurement

The access terminal shall measure the strength of every pilot it searches. The strength estimate formed by the access terminal shall be computed as the sum of the ratios of received pilot energy per chip, E_c, to total received spectral density, I_0 (signal and noise) for at most k multipath components, where k is the maximum number of multipath components that can be demodulated simultaneously by the access terminal.

6.6.5.3.4 Pilot Drop Timer Maintenance

For each pilot, the access terminal shall maintain a pilot drop timer.

If DynamicThresholds is equal to '0', the access terminal shall start a pilot drop timer for each pilot in the Candidate Set or the Active Set whenever the strength becomes less than the value specified by PilotDrop. The access terminal shall set the timer value to expired after the time specified by PilotDropTimer. The timer shall be reset and disabled if, before it expires, the strength of the pilot becomes greater than the value specified by PilotDrop.

If DynamicThresholds is equal to '1', the access terminal shall perform the following:

- The access terminal shall start a pilot drop timer for each pilot in the Candidate Set whenever the strength of the pilot becomes less than the value specified by PilotDrop and the pilot drop timer shall be set to expired after the time specified by PilotDropTimer. The timer shall be reset and disabled if the strength of the pilot becomes greater than the value specified by PilotDrop before it expires.
- For each pilot in the Active Set, the access terminal shall sort pilots in the Active Set in order of increasing strengths, i.e., $PS_1 < PS_2 < PS_3 < \ldots < PS_{N_A}$, where N_A is the number of the pilots in the Active Set. The access terminal shall start the timer whenever the strength PS_i satisfies the following inequality:

$$10 \times \log_{10} PS_i < \max\left(\frac{\text{SoftSlope}}{8} \times 10 \times \log_{10} \sum_{j>i} PS_j + \frac{\text{DropIntercept}}{2}, -\frac{\text{PilotDrop}}{2}\right)$$

$$i = 1, 2, \ldots, N_A - 1$$

The access terminal shall reset and disable the timer whenever the above inequality is not satisfied for the corresponding pilot.

Sections 6.6.5.3.6 and 6.6.5.6.3 specify the actions the access terminal takes when the pilot drop timer expires.

6.6.5.3.5 Active Set Management

The access terminal shall support a maximum Active Set size of $N_{RUPActive}$ pilots.

Rules for maintaining the Active Set are specific to each protocol state (see 6.6.5.5.1 and 6.6.5.6.1).

6.6.5.3.6 Candidate Set Management

The access terminal shall support a maximum Candidate Set size of $N_{RUPCandidate}$ pilots.

The access terminal shall add a pilot to the Candidate Set if one of the following conditions is met:

- Pilot is not already in the Active Set or Candidate Set and the strength of the pilot exceeds the value specified by PilotAdd.
- Pilot is deleted from the Active Set, its pilot drop timer has expired, DynamicThresholds is equal to '1', and the pilot strength is above the threshold specified by PilotDrop.
- Pilot is deleted from the Active Set but its pilot drop timer has not expired.

The access terminal shall delete a pilot from the Candidate Set if one of the following conditions is met:

- Pilot is added to the Active Set.
- Pilot's drop timer has expires.
- Pilot is added to the Candidate Set; and, as a consequence, the size of the Candidate Set exceeds $N_{RUPCandidate}$. In this case, the access terminal shall delete the weakest pilot in the set. Pilot A is considered weaker than pilot B:
  - If pilot A has an active drop timer but pilot B does not,
  - If both pilots have an active drop timer and pilot A's drop timer is closer to expiration than pilot B's, or
  - If neither of the pilots has an active drop timer and pilot A's strength is less than pilot B's.

6.6.5.3.7 Neighbor Set Management

The access terminal shall support a minimum Neighbor Set size of $N_{RUPNeighbor}$ pilots.

Upon receiving the first ***OverheadMessages.Updated*** indication since transitioning out of the Inactive State, the access terminal shall initialize the Neighbor Set to the list of neighbors pilots given as public data by the Overhead Messages Protocol.

The access terminal shall implement a "least recently used" scheme for pilots in the Neighbor Set as follows.

The access terminal shall maintain a counter, AGE, for each pilot in the Neighbor Set. The initial setting of this counter depends on what set the pilot was in before it became a member of the Neighbor Set:

- For pilots that were deleted from the Active Set or Candidate Set, the access terminal shall set AGE to 0 when adding these pilots to the Neighbor Set.
- For pilots that were deleted from the Remaining Set, the access terminal shall set AGE to NeighborMaxAge when adding these pilots to the Neighbor Set.
- When the access terminal initializes the Neighbor Set, it shall set AGE to NeighborMaxAge for each pilot in the set.

The access terminal shall increment AGE for every pilot in the Neighbor Set each time either of the following occurs:

- The access terminal receives an ***OverheadMessages.Updated*** indication and the public data of the Overhead Messages Protocol contains a neighbor list that is not identical to the list provided previously as public data by the Overhead Messages Protocol , or
- The access terminal receives a NeighborList message listing a neighbor list that is not identical to the list specified in the previous (if any) NeighborList message.

The access terminal shall add a pilot to the Neighbor Set if:

- The pilot was deleted from the Active Set with an expired pilot drop timer.
- The pilot drop timer of a pilot in the Candidate Set expires.
- The pilot was a member of the Remaining Set, and it was either provided as public data by the Overhead Messages Protocol or it was listed in a received NeighborList message. The access terminal shall add the pilots listed in the message in the order they are listed, and shall only add the pilots to the Neighbor Set if, after adding them and deleting the appropriate pilots, the size of the Neighbor Set does not exceed $N_{RUPNeighbor}$.

The access terminal shall delete a pilot from the Neighbor Set if:

- The Pilot is added to the Active Set or Candidate Set, or if the AGE of the pilot exceeds NeighborMaxAge and the size of the Neighbor Set exceeds $N_{RUPNeighbor}$ due to new additions.

If there are more pilots with AGE exceeding NeighborMaxAge than needed to make room for new additions to the Neighbor Set, the pilot with the highest AGE shall be deleted first.

The access terminal shall perform the procedures specified in 6.6.5.3.1 if a plot (specified by the pilot's PN offset and the pilot's CDMA Channel) is added to or deleted from the Neighbor Set.

6.6.5.3.8 Remaining Set Management

The access terminal shall initialize the Remaining Set to contain all the pilots whose PN offset index is an integer multiple of PilotIncrement and are not already members of any other set.

The access terminal shall add a pilot to the Remaining Set if it deletes the pilot from the Neighbor Set and if the pilot was not added to the Active Set or Candidate Set.

The access terminal shall delete the pilot from the Remaining Set if it adds it to another set.

6.6.5.3.9 Pilot PN Phase Measurement

The access terminal shall measure the arrival time, PILOT_ARRIVAL, for each pilot reported to the access network. The pilot arrival time shall be the time of occurrence, as measured at the access terminal antenna connector, of the earliest arriving usable multipath component of the pilot. The arrival time shall be measured relative to the access terminal's time reference in units of PN chips. The access terminal shall compute the reported pilot PN phase, PILOT_PN_PHASE, as:

$$\text{PILOT\_PN\_PHASE} = (\text{PILOT\_ARRIVAL} + (64 \times \text{PILOT\_PN})) \bmod 2^{15},$$

where PILOT_PN is the PN sequence offset index of the pilot.

6.6.5.4 Message Sequence Numbers

The access network shall validate all received RouteUpdate messages as specified in 6.6.5.4.1.

The access terminal shall validate all received TrafficChannelAssignment messages as specified in 6.6.5.4.2.

The RouteUpdate message and the TrafficChannelAssignment message carry MessageSequence field that serves to flag duplicate or stale messages.

The MessageSequence field of the RouteUpdate message is independent of the MessageSequence field of the TrafficChannelAssignment message.

6.6.5.4.1 RouteUpdate Message Validation

When the access terminal first sends a RouteUpdate message, it shall set the MessageSequence field of the message to zero. Subsequently, the access terminal shall increment this field each time it sends a RouteUpdate message.

The access network shall consider all RouteUpdate messages it receives in the Idle State as valid.

The access network shall initialize the receive pointer, ***V(R)*** to the MessageSequence field of the first RouteUpdate message it received in the Idle State, and the access network shall subsequently set it to the MessageSequence field of each received RouteUpdate message.

When the access network receives a RouteUpdate message in the Connected State, it shall validate the message using the procedure defined in 10.6. The access network shall discard the message if it is stale.

6.6.5.4.2 TrafficChannelAssignment Message Validation

The access network shall set the MessageSequence field of the TrafficChannelAssignment message it sends in the Idle State to zero. Subsequently, each time the access network sends a new TrafficChannelAssignment message in the Connected State, it shall increment this field. If the access network is sending the same message multiple times, it shall not change the value of this field between transmissions.[23]

The access terminal shall initialize a receive pointer, ***V(R)*** to the MessageSequence field of the TrafficChannelAssignment message that it receives in the Idle State.

When the access terminal receives a TrafficChannelAssignment message, it shall validate the message using the procedure defined in 10.6. The access terminal shall discard the message if it is stale.

6.6.5.5 Idle State

The Idle State corresponds to the Air Link Management Protocol Idle State.

In this state, RouteUpdate messages from the access terminal are based on the distance between the sector where the access terminal last sent a RouteUpdate message and the sector currently in its active set.

The access network sends the TrafficChannelAssignment message to open a connection in this state.

Upon entering this state, the access terminal shall remove all Neighbor structures from NeighborListMessageNeighborList and perform the procedures specified in 6.6.5.3.1.

6.6.5.5.1 Active Set Maintenance

The access network shall not initially maintain an Active Set for the access terminal in this state.

If the access network receives an ***Open*** command, it shall initialize the Active Set to the set of pilots it sends in the TrafficChannelAssignment message, sent in response to the command (see 6.6.5.2.3).

The access terminal shall initially keep an Active Set of size one when it is in the Idle State. The Active Set pilot shall be the pilot associated with the Control Channel the access terminal is currently monitoring. The access terminal shall send an ***IdleHO*** indication when the Active Set changes in the Idle State.

[23] The access network may send a message multiple times to increase its delivery probability.

The access terminal shall not change its Active Set pilot at a time that causes it to miss a synchronous Control Channel capsule. Other rules governing when to replace this Active Set pilot are beyond the scope of this specification.

If the access terminal receives a TrafficChannelAssignment message, it shall set its Active Set to the list of pilots specified in the message.

6.6.5.5.2 Pilot Channel Supervision in the Idle State

The access terminal shall perform pilot channel supervision in the Idle State as follows:

- Access terminal shall monitor the pilot strength of the pilot in its active set, all the pilots in the candidate set and all the pilots in the neighbor set that are on the same frequency.
- If the strength of all the pilots that the access terminal is monitoring goes below the value specified by PilotDrop, the access terminal shall start a pilot supervision timer for $T_{RUPPilotSupervision}$ seconds.
- If the strength of at least one of the pilots goes above the value specified by PilotDrop while the pilot supervision timer is counting down, the access terminal shall stop the timer.
- If the pilot supervision timer expires, the access terminal shall return a ***NetworkLost*** indication.

6.6.5.5.3 Processing the TrafficChannelAssignment Message in the Idle State

If the access terminal receives a TrafficChannelAssignment message in this state, it shall update its Active Set as described above, and perform the following:

- If the Channel Record is included in the message, the access terminal shall set CurrentFrequency to the current CDMA channel.
- Start a connection timer for $T_{RUPConnectionSetup}$ seconds.
- Issue the following commands:
  - ***ReverseTrafficChannelMAC.Activate***
  - ***ForwardTrafficChannelMAC.Activate***
- If the protocol receives a ***ReverseTrafficChannelMAC.LinkAcquired*** indication the access terminal shall:
  - Send a TrafficChannelComplete message with the MessageSequence field of the message set to the MessageSequence field of the TrafficChannelAssignment message.
  - Disable the connection timer.
  - Transition to the Connected State.

If the connection timer expires the access terminal shall perform the following:

- Issue a ***ReverseTrafficChannelMAC.Deactivate*** command.

- Issue a ***ForwardTrafficChannelMAC.Deactivate*** command.
- If as a result of processing the TrafficChannelAssignment message the access terminal has tuned to a different frequency, the access terminal shall return back to the frequency that is was monitoring prior to processing of the TrafficChannelAssignment message.

6.6.5.5.4 Route Update Report Rules

The access terminal shall send RouteUpdate messages to update its location with the access network.

The access terminal shall not send a RouteUpdate message if the connection timer is active.

The access terminal shall comply with the following rules when sending RouteUpdate messages.

- The access terminal shall send a RouteUpdate message whenever it transmits on the Access Channel.
- The access terminal shall include in the RouteUpdate message the pilot PN phase, pilot strength, and drop timer status for every pilot in the Active Set and Candidate Set.
- The access terminal shall send a RouteUpdate message if the computed value ***r*** is greater than the value provided in the RouteUpdateRadius field of the SectorParameters message transmitted by the sector in which the access terminal last sent a RouteUpdate message.

  If (x_L,y_L) are the longitude and latitude of the sector in whose coverage area the access terminal last sent a RouteUpdate, and (x_C,y_C) are the longitude and latitude of the sector currently providing coverage to the access terminal, then ***r*** is given by[24]

$$r = \left\lfloor \frac{\sqrt{\left[(x_C - x_L)\times\cos\left(\frac{p}{180}\times\frac{y_L}{14400}\right)\right]^2 + [y_C - y_L]^2}}{16} \right\rfloor$$

The access terminal shall compute ***r*** with an error of no more than ±5% of its true value when $|y_L/14400|$ is less than 60 and with an error of no more than ±7% of its true value when $|y_L/14400|$ is between 60 and 70.[25]

[24] The ***x's*** denote longitude and the ***y's*** denote latitude.

[25] x_L and y_L are given in units of 1/4 seconds. $x_L/14400$ and $y_L/14400$ are in units of degrees.

6.6.5.6 Connected State

The Connected State corresponds to the Air Link Management Protocol Connected State.

In this state, RouteUpdate messages from the access terminal are based on changes in the radio link between the access terminal and the access network, obtained through pilot strength measurements at the access terminal.

The access network determines the contents of the Active Set through TrafficChannelAssignment messages.

6.6.5.6.1 Active Set Maintenance

6.6.5.6.1.1 Access Network

Whenever the access network sends a TrafficChannelAssignment message to the access terminal, it shall add to the Active Set any pilots listed in the message that are not currently in the Active Set.

The access network shall delete a pilot from the Active Set if the pilot was not listed in a TrafficChannelAssignment message and if the access network received the TrafficChannelComplete message, acknowledging that TrafficChannelAssignment message.

The access network should send a TrafficChannelAssignment message to the access terminal in response to changing radio link conditions, as reported in the access terminal's RouteUpdate messages.

The access network should only specify a pilot in the TrafficChannelAssignment message if it has allocated the required resources in the associated sector. This means that the sector specified by the pilot is ready to receive data from the access terminal and is ready to transmit queued data to the access terminal should the access terminal point its DRC at that sector.

If the access network adds or deletes a pilot in the Active Set, it shall send an *ActiveSetUpdated* indication.

If the access network adds a pilot specified in a RouteUpdate message to the Active Set, the access network may use the PilotPNPhase field provided in the message to obtain a round trip delay estimate from the access terminal to the sector associated with this pilot. The access network may use this estimate to accelerate the acquisition of the access terminal's Reverse Traffic Channel in that sector.

6.6.5.6.1.2 Access Terminal

If the access terminal receives a valid TrafficChannelAssignment message (see 6.6.5.4.2), it shall replace the contents of its current Active Set with the pilots specified in the message. The access terminal shall process the message as defined in 6.6.5.6.4.

6.6.5.6.2 ResetReport Message

The access network may send a ResetReport message to reset the conditions under which RouteUpdate messages are sent from the access terminal. Access terminal usage of the ResetReport message is specified in the following section.

6.6.5.6.3 Route Update Report Rules

The access terminal sends a RouteUpdate message to the access network in this state to request addition or deletion of pilots from its Active Set. The access terminal shall send the message if any one of the following occurs:

- If DynamicThresholds is equal to '0' and the strength of a Neighbor Set or Remaining Set pilot is greater than the value specified by PilotAdd.
- If DynamicThresholds is equal to '1' and the strength of a Neighbor Set or Remaining Set pilot, PS, satisfies the following inequality:

$$10\times\log_{10}PS > \max\left(\frac{\text{SoftSlope}}{8}\times 10\times\log_{10}\sum_{i\in A}PS_i+\frac{\text{AddIntercept}}{2}, -\frac{\text{PilotAdd}}{2}\right)$$

  where the summation is performed over all pilots currently in the Active Set.

- If DynamicThresholds is equal to '0' and the strength of a Candidate Set pilot is greater than the value specified by PilotCompare above an Active Set pilot, and a RouteUpdate message carrying this information has not been sent since the last ResetReport message was received.
- If DynamicThresholds is equal to '1' and
  - the strength of a Candidate Set pilot, PS, satisfies the following inequality:

$$10\times\log_{10}PS > \frac{\text{SoftSlope}}{8}\times 10\times\log_{10}\sum_{i\in A}PS_i+\frac{\text{AddIntercept}}{2}$$

    where the summation is performed over all pilots currently in the Active Set, and
  - a RouteUpdate message carrying this information has not been sent since the last ResetReport message was received.
- If DynamicThresholds is equal to '1' and
  - the strength of a Candidate Set pilot is greater than the value specified by PilotCompare above an Active Set pilot, and
  - the strength of a Candidate Set pilot, PS, satisfies the following inequality:

$$10\times\log_{10}PS > \frac{\text{SoftSlope}}{8}\times 10\times\log_{10}\sum_{i\in A}PS_i+\frac{\text{AddIntercept}}{2}$$

    where the summation is performed over all pilots currently in the Active Set, and

  - a RouteUpdate message carrying this information has not been sent since the last ResetReport message was received.

- The pilot drop timer of an Active Set pilot has expired, and a RouteUpdate message carrying this information has not been sent since the last ResetReport message was received.

6.6.5.6.4 Processing the TrafficChannelAssignment Message

The access terminal shall process a valid TrafficChannelAssignment (see 6.6.5.4.2) message as follows:

- If the TrafficChannelAssignment message contains a value for the FrameOffset that is different from the value of the FrameOffset received in the last TrafficChannelAssignment message that was received in the Idle state, then the access terminal shall return a ***RouteUpdate.AssignmentRejected*** indication and shall discard the message.
- The access terminal shall update its Active Set as defined in 6.6.5.6.1.2.
- The access terminal shall tune to the frequency defined by the Channel record, if this record is included in the message.
- The access terminal shall start monitoring and responding to the Power Control Channels defined by the MACIndex fields provided in the message. The access terminal should use the SofterHandoff fields to identify the Power Control Channels that are carrying identical information and can therefore be soft-combined.
- The access terminal shall send the access network a TrafficChannelComplete message specifying the MessageSequence value received in the TrafficChannelAssignment message.

6.6.5.6.5 Processing the TrafficChannelComplete Message

The access network should set a transaction timer when it sends TrafficChannelAssignment message. If the access network sets a transaction timer, it shall reset the timer when it receives a TrafficChannelComplete message containing a MessageSequence field equal to the one sent in the TrafficChannelAssignment message.

If the timer expires, the access network should return a ***RouteUpdate.ConnectionLost*** indication.

6.6.5.6.6 Transmission and Processing of the NeighborList Message

The access network may send the NeighborList message to the access terminal when the protocol is in the Connected State to override the search window size and/or search window offset corresponding to a pilot in the Neighbor Set.

Upon receiving a NeighborList message, the access terminal shall perform the following in the order specified:

- The access terminal shall remove all Neighbor structures from NeighborListMessageNeighborList.
- For each pilot (specified by its pilot PN and its channel) listed in the received NeighborList message, the access terminal shall add a Neighbor structure to NeighborListMessageNeighborList and populate it as follows:
  - Set the structure's PilotPN field to the message's corresponding PilotPN field.
  - If the message's ChannelIncluded field is set to '1', set the structure's Channel field to the message's corresponding Channel field. Otherwise, set the structure's Channel field to the current channel.
  - If the message's SearchWindowSizeIncluded field is set to '1', then set the structure's SearchWindowSize field to the message's corresponding SearchWindowSize field. Otherwise, set the structure's SearchWindowSize field to NULL.
  - If the SearchWindowOffsetIncluded field is set to '1', then set the structure's SearchWindowOffset field to the message's corresponding SearchWindowOffset field. Otherwise, set the structure's SearchWindowOffset field to NULL.
- Perform the procedures specified in 6.6.5.3.1.

6.6.5.6.7 Processing of OverheadMessages.Updated Indication

Upon receiving ***OverheadMessages.Updated*** indication, the access terminal shall perform the following:

- The access terminal shall remove all Neighbor structures from the OverheadMessagesNeighborList list.
- For each pilot (specified by its pilot PN and its channel) in the neighbor list given as public data of Overhead Messages Protocol, the access terminal shall add a Neighbor structure to the OverheadMessagesNeighborList list and populate it as follows:
  - Set the structure's PilotPN field to the corresponding NieghborPilotPN field given as public data of the Overhead Messages Protocol.
  - If the Overhead Messages Protocol's NeighborChannelIncluded field is set to '1', set the structure's Channel field to the Overhead Messages Protocol's corresponding NeighborChannel. Otherwise, set the structure's Channel field to the current channel.
  - If the Overhead Messages Protocol's SearchWindowSizeIncluded field is set to '1', then set the structure's SearchWindowSize field to the Overhead Messages Protocol's corresponding SearchWindowSize field. Otherwise, set the structure's SearchWindowSize field to NULL.
  - If the Overhead Messages Protocol's SearchWindowOffsetIncluded field is set to '1', then set the structure's SearchWindowOffset field to the Overhead Messages Protocol's corresponding SearchWindowOffset field. Otherwise, set the structure's SearchWindowOffset field to NULL.

- Perform the procedures specified in 6.6.5.3.1.

6.6.6 Message Formats

6.6.6.1 RouteUpdate

The access terminal sends the RouteUpdate message to notify the access network of its current location and provide it with an estimate of its surrounding radio link conditions.

Field	Length (bits)
MessageID	8
MessageSequence	8
ReferencePilotPN	9
ReferencePilotStrength	6
ReferenceKeep	1
NumPilots	4

NumPilots occurrences of the following three fields:

PilotPNPhase	15
ChannelIncluded	1
Channel	0 or 24
PilotStrength	6
Keep	1

Reserved	Variable

MessageID The access terminal shall set this field to 0x00.

MessageSequence The access terminal shall set this field to the sequence number of this message. The sequence number of this message is 1 more than the sequence number of the last RouteUpdate message (modulo 2^8) sent by this access terminal. If this is the first RouteUpdate message sent by the access terminal, it shall set this field to 0x00.

ReferencePilotPN The access terminal shall set this field to the access terminal's time reference (the reference pilot), relative to the zero offset pilot PN sequence in units of 64 PN chips.

ReferencePilotStrength

The access terminal shall set this field to $\lfloor -2 \times 10 \times \log_{10} PS \rfloor$, where PS is the strength of the reference pilot, measured as specified in 6.6.5.3.2. If this value is less than 0, the access terminal shall set this field to '000000'. If this value is greater than '111111', the access terminal shall set this field to '111111'.

ReferenceKeep

If the pilot drop timer corresponding to the reference pilot has expired, the access terminal shall set this field to '0'; otherwise, the access terminal shall set this field to '1'.

NumPilots

The access terminal shall set this field to the number of pilots that follow this field in the message.

PilotPNPhase

The PN offset in resolution of 1 chip of a pilot in the Active Set or Candidate Set of the access terminal that is not the reference pilot.

ChannelIncluded

The access terminal shall set this field to '1' if the channel for this pilot offset is not the same as the current channel. Otherwise, the access terminal shall set this field to '0'.

Channel

The access terminal shall include this field if the ChannelIncluded field is set to '1'. The access terminal shall set this to the channel record corresponding to this pilot (see 10.1). Otherwise, the access terminal shall omit this field for this pilot offset.

PilotStrength

The access terminal shall set this field to $\lfloor -2 \times 10 \times \log_{10} PS \rfloor$, where PS is the strength of the pilot in the above field, measured as specified in 6.6.5.3.2. If this value is less than 0, the access terminal shall set this field to '000000'. If this value is greater than '111111', the access terminal shall set this field to '111111'.

Keep

If the pilot drop timer corresponding to the pilot in the above field has expired, the access terminal shall set this field to '0'; otherwise, the access terminal shall set this field to '1'.

Reserved

The number of bits in this field is equal to the number needed to make the message length an integer number of octets. This field shall be set to all zeros.

Channels	AC	RTC
Addressing		unicast

SLP	Reliable[26]	Best Effort
Priority	20	

6.6.6.2 TrafficChannelAssignment

The access network sends the TrafficChannelAssignment message to manage the access terminal's Active Set.

Field	Length (bits)
MessageID	8
MessageSequence	8
ChannelIncluded	1
Channel	0 or 24
FrameOffset	4
DRCLength	2
DRCChannelGain	6
AckChannelGain	6
NumPilots	4

NumPilots occurrences of the following fields

PilotPN	9
SofterHandoff	1
MACIndex	6
DRCCover	3
RABLength	2
RABOffset	3

Reserved	Variable

MessageID The access network shall set this field to 0x01.

[26] This message is sent reliably when it is sent over the Reverse Traffic Channel.

MessageSequence The access network shall set this to 1 higher than the MessageSequence field of the last TrafficChannelAssignment message (modulo 2^S, S = 8) sent to this access terminal.

ChannelIncluded The access network shall set this field to '1' if the Channel record is included for these pilots. Otherwise, the access network shall set this field to '0'.

Channel The access network shall include this field if the ChannelIncluded field is set to '1'. The access network shall set this to the channel record corresponding to this pilot (see 10.1). Otherwise, the access network shall omit this field for this pilot offset. If Channel is included, the access network shall set the SystemType field of the Channel record to '0000'.

FrameOffset The access network shall set this field to the frame offset the access terminal shall use when transmitting the Reverse Traffic Channel, in units of slots.

DRCLength The access network shall set this field to the number of slots the access terminal shall use to transmit a single DRC value, as shown in Table 6.6.6.2-1.

Table 6.6.6.2-1. DRCLength Encoding

Field value (binary)	DRCLength (slots)
'00'	1
'01'	2
'10'	4
'11'	8

DRCChannelGain The access network shall set this field to the ratio of the power level of the DRC Channel (when it is transmitted) to the power level of the Reverse Traffic Pilot Channel expressed as 2's complement value in units of 0.5 dB. The valid range for this field is from –9 dB to +6 dB, inclusive. The access terminal shall support all the values in the valid range for this field.

AckChannelGain The access network shall set this field to the ratio of the power level of the Ack Channel (when it is transmitted) to the power level of the Reverse Traffic Pilot Channel expressed as 2's complement value in units of 0.5 dB. The valid range for this field is from –3 dB to +6 dB, inclusive. The access terminal shall support the all the values in valid range for this field.

NumPilots The access network shall set this field to the number of pilots included in this message.

PilotPN The access network shall set this field to the PN Offset associated with the sector that will transmit a Power Control Channel to the access terminal, to whom the access terminal is allowed to point its DRC, and whose Control Channel and Forward Traffic Channel the access terminal may monitor.

SofterHandoff If the Forward Traffic Channel associated with this pilot will carry the same closed-loop power control bits as that of the previous pilot in this message, the access network shall set this field to '1'; otherwise, the access network shall set this field to '0'. The access network shall set the first instance of this field to '0'.

MACIndex Medium Access Control Index. The access network shall set this field to the MACIndex assigned to the access terminal by this sector.

DRCCover The access network shall set this field to the index of the DRC cover associated with the sector specified in this record.

RABLength The access network shall set this field to the number of slots over which the Reverse Activity Bit is transmitted, as shown in Table 6.6.6.2-2.

Table 6.6.6.2-2. Encoding of the RABLength Field

Field value (binary)	RABLength (slots)
'00'	8
'01'	16
'10'	32
'11'	64

RABOffset The access network shall set this field to indicate the slots in which a new Reverse Activity Bit is transmitted by this sector. The value (in slots) of RABOffset is the number the field is set to multiplied by RABLength/8.

Reserved The number of bits in this field is equal to the number needed to make the message length an integer number of octets. This field shall be set to all zeros.

Channels	CC FTC
Addressing	unicast

SLP	Reliable Best Effort[27]
Priority	20

6.6.6.3 TrafficChannelComplete

The access terminal sends the TrafficChannelComplete message to provide an acknowledgement for the TrafficChannelAssignment message.

Field	Length (bits)
MessageID	8
MessageSequence	8

MessageID The access terminal shall set this field to 0x02.

MessageSequence The access terminal shall set this field to the MessageSequence field of the TrafficChannelAssignment message whose receipt this message is acknowledging.

Channels	RTC
Addressing	unicast

SLP	Reliable
Priority	40

6.6.6.4 ResetReport

The access network sends the ResetReport message to reset the RouteUpdate transmission rules at the access terminal.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x03.

[27] The TrafficChannelAssignment message sent in response to the Open command is sent using best effort SLP. All subsequent TrafficChannelAssignment messages are sent using reliable delivery SLP.

Channels	FTC	SLP	Reliable
Addressing	unicast	Priority	40

6.6.6.5 NeighborList

The NeighborList message is used to convey information corresponding to the neighboring sectors to the access terminals when the access terminal is in the Connected State.

Field	Length (bits)
MessageID	8
Count	5

Count occurrences of the following field:

PilotPN	9

Count occurrences of the following two fields:

ChannelIncluded	1
Channel	0 or 24

SearchWindowSizeIncluded	1

Count occurrences of the following field

SearchWindowSize	0 or 4

SearchWindowOffsetIncluded	1

Count occurrences of the following field

SearchWindowOffset	0 or 3

Reserved	Variable

MessageID The access network shall set this field to 0x04.

Count The access network shall set this field to the number of records specifying neighboring sectors information included in this message.

PilotPN

The access network shall set this field to the PN Offset of neighboring sector for which the access network is providing search window information in this message.

ChannelIncluded

The access network shall set this field to ‘1’ if a Channel record is included for this neighbor, and to ‘0’ otherwise. The access network shall omit this field if the corresponding NeighborChannelIncluded field is set to ‘0’. Otherwise, if included, the n^{th} occurrence of this field corresponds to the n^{th} occurrence of PilotPN in the record that contains the PilotPN field above.

Channel

Channel record specification for the neighbor channel. See 10.1 for the Channel record format. The n^{th} occurrence of this field corresponds to the n^{th} occurrence of PilotPN in the record that contains the PilotPN field above.

SearchWindowSizeIncluded

The access network shall set this field to ‘1’ if SeachWindowNeighbor field for neighboring sectors is included in this message. Otherwise, the access network shall set this field to ‘0’.

SearchWindowSize

The access network shall omit this field if SearchWindowSizeIncluded is set to ‘0’. If SearchWindowSizeIncluded is set to ‘1’, the access network shall set this field to the value shown in Table 6.6.6.5-1 corresponding to the search window size to be used by the access terminal for the neighbor pilot. The n^{th} occurrence of this field corresponds to the n^{th} occurrence of PilotPN in the record that contains the PilotPN field above.

Table 6.6.6.5-1. Search Window Sizes

SearchWindowSize Value	Search Window Size (PN chips)
0	4
1	6
2	8
3	10
4	14
5	20
6	28
7	40
8	60
9	80
10	100
11	130
12	160
13	226
14	320
15	452

SearchWindowOffsetIncluded

The access network shall set this field to '1' if SeachWindowOffset field for neighboring sectors is included in this message. Otherwise, the access network shall set this field to '0'.

SeachWindowOffsetIncluded

The access network shall omit this field if SearchWindowOffsetIncluded is set to '0'. If SearchWindowOffsetIncluded is set to '1', the access network shall set this field to the value shown in Table 6.6.6.5-2 corresponding to the search window offset to be used by the access terminal for the neighbor pilot. The n^{th} occurrence of this field corresponds to the n^{th} occurrence of PilotPN in the record that contains the PilotPN field above.

Table 6.6.6.5-2. Search Window Offset

SearchWindowOffset	Offset (PN chips)
0	0
1	WindowSize[28] /2
2	WindowSize
3	3 × WindowSize /2
4	- WindowSize /2
5	- WindowSize
6	-3 × WindowSize /2
7	Reserved

Reserved The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC	FTC
Addressing		unicast

SLP	Reliable
Priority	40

6.6.6.5 Configuration Messages

The Default Route Update Protocol uses the Generic Configuration Protocol to transmit configuration parameters from the access network to the access terminal. The following messages are defined:

6.6.6.5.1 ConfigurationRequest

The access network sends the ConfigurationRequest message to override the defaults used by the access terminal for a number of protocol parameters. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The access network shall use a complex attribute (see 10.3) in the ConfigurationRequest message.

The access network shall set the MessageID field of this message to 0x50.

[28] WindowSize is pilot's search window size in PN chips.

The access network shall use the complex attributes defined in 6.6.6.5.1.1, 6.6.6.5.1.2, and 6.6.6.5.1.3when sending the ConfigurationRequest message. If the access terminal does not receive a ConfigurationRequest message, it shall use the following default values.

Channels	CC FTC
Addressing	unicast

SLP	Best Effort
Priority	60

6.6.6.5.1.1 SearchParameters Attribute

Field	Length (bits)	Default Value
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PilotIncrement	4	4
SearchWindowActive	4	8
SearchWindowNeighbor	4	10
SearchWindowRemaining	4	10

Length Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID The access network shall set this field to 0x00.

ValueID This field identifies this particular set of values for the attribute. The access network shall increment this field for each complex attribute-value record for a particular attribute.

PilotIncrement The access network shall set this field to the pilot PN sequence increment, in units of 64 PN chips, that access terminals are to use for searching the Remaining Set. The access network should set this field to the largest increment such that the pilot PN sequence offsets of all its neighbor access networks are integer multiples of that increment. The access terminal shall support all the valid values for this field.

SearchWindowActive

Search window size for the Active Set and Candidate Set. The access network shall set this field to the value shown in Table 6.6.6.5-1 corresponding to the search window size to be used by the access terminal for the Active Set and Candidate Set. The access terminal shall support all the valid values specified by this field.

SearchWindowNeighbor

Search window size for the Neighbor Set. The access network shall set this field to the value shown in Table 6.6.6.5-1 corresponding to the search window size to be used by the access terminal for the Neighbor Set. The access terminal shall support all the valid values specified by this field.

SearchWindowRemaining

Search window size for the Remaining Set. The access network shall set this field to the value shown in Table 6.6.6.5-1 corresponding to the search window size to be used by the access terminal for the Remaining Set. The access terminal shall support all the valid values specified by this field.

6.6.6.5.1.2 SetManagementSameChannelParameters Attribute

The access terminal shall use these attributes if the pilot being compared is on the same channel as the active set pilots' channel.

Field	Length (bits)	Default Value
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PilotAdd	6	0x0e
PilotCompare	6	0x05
PilotDrop	6	0x12
PilotDropTimer	4	3
DynamicThresholds	1	0
SoftSlope	0 or 6	N/A
AddIntercept	0 or 6	N/A
DropIntercept	0 or 6	N/A
NeighborMaxAge	4	0
Reserved	variable	N/A

Length — Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — The access network shall set this field to 0x01.

ValueID — This field identifies this particular set of values for the attribute. The access network shall increment this field for each complex attribute-value record for a particular attribute.

PilotAdd — This value is used by the access terminal to trigger a RouteUpdate in the Connected State. The access network shall set this field to the pilot detection threshold, expressed as an unsigned binary number equal to $\lfloor - 2 \times 10 \times \log 10\ Ec/I_0 \rfloor$. The value used by the access terminal is –0.5 dB times the value of this field. The access terminal shall support all the valid values specified by this field.

PilotDrop — This value is used by the access terminal to start a pilot drop timer for a pilot in the Active Set or the Candidate Set. The access network shall set this field to the pilot drop threshold, expressed as an unsigned binary number equal to $\lfloor - 2 \times 10 \times \log 10\ Ec/I_0 \rfloor$. The value used by the access terminal is –0.5 dB times the value of this field.

The access terminal shall support all the valid values specified by this field.

PilotCompare Active Set versus Candidate Set comparison threshold, expressed as a 2's complement number. The access terminal transmits RouteUpdate message when the strength of a pilot in the Candidate Set exceeds that of a pilot in the Active Set by this margin. The access network shall set this field to the threshold Candidate Set pilot to Active Set pilot ratio, in units of 0.5 dB. The access terminal shall support all the valid values specified by this field.

PilotDropTimer Timer value after which an action is taken by the access terminal for a pilot that is a member of the Active Set or Candidate Set, and whose strength has not become greater than the value specified by PilotDrop. If the pilot is a member of the Active Set, a RouteUpdate message is sent in the Connected State. If the pilot is a member of the Candidate Set, it will be moved to the Neighbor Set. The access network shall set this field to the drop timer value shown in Table 6.6.6.5.1-1 corresponding to the pilot drop timer value to be used by access terminals. The access terminal shall support all the valid values specified by this field.

Table 6.6.6.5.1-1. Pilot Drop Timer Values

PilotDropTimer	Timer Expiration (seconds)	PilotDropTimer	Timer Expiration (seconds)
0	< 0.1	8	27
1	1	9	39
2	2	10	55
3	4	11	79
4	6	12	112
5	9	13	159
6	13	14	225
7	19	15	319

DynamicThresholds This field shall be set to '1' if the following three fields are included in this record. Otherwise, this field shall be set to '0'.

SoftSlope This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to an unsigned binary number, which is used by the access terminal in the inequality criterion for adding a pilot to the Active Set or dropping a pilot from the Active Set. The access terminal shall support all the valid values specified by this field.

AddIntercept This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to a 2's complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.

DropIntercept This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to a 2's complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.

NeighborMaxAge The access network shall set this field to the maximum AGE value beyond which the access terminal is to drop members from the Neighbor Set. The access terminal shall support all the valid values specified by this field.

Reserved The access network shall set this field to zero. The access terminal shall ignore this field. The length of this field shall be such that the entire record is octet-aligned.

6.6.6.5.1.3 SetManagementDifferentChannelParameters Attribute

The access terminal shall use these attributes if the pilot being compared is on a channel that is different from the active set pilots' channel.

Field	Length (bits)	Default Value
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PilotAdd	6	0x0e
PilotCompare	6	0x05
PilotDrop	6	0x12
PilotDropTimer	4	3
DynamicThresholds	1	0
SoftSlope	0 or 6	N/A
AddIntercept	0 or 6	N/A
DropIntercept	0 or 6	N/A
NeighborMaxAge	4	0
Reserved	variable	N/A

Length Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID The access network shall set this field to 0x02.

ValueID This field identifies this particular set of values for the attribute. The access network shall increment this field for each complex attribute-value record for a particular attribute.

PilotAdd This value is used by the access terminal to trigger a RouteUpdate in the Connected State. The access network shall set this field to the pilot detection threshold, expressed as an unsigned binary number equal to $\lfloor - 2 \times 10 \times \log10\ Ec/I_0 \rfloor$. The value used by the access terminal is –0.5 dB times the value of this field. The access terminal shall support all the valid values specified by this field.

PilotDrop This value is used by the access terminal to start a pilot drop timer for a pilot in the Active Set or the Candidate Set. The access network shall set this field to the pilot drop threshold, expressed as an unsigned binary number equal to $\lfloor - 2 \times 10 \times \log10\ Ec/I_0 \rfloor$. The value used by the access terminal is –0.5 dB times the value of this field.

The access terminal shall support all the valid values specified by this field.

PilotCompare Active Set versus Candidate Set comparison threshold, expressed as a 2's complement number. The access terminal transmits RouteUpdate message when the strength of a pilot in the Candidate Set exceeds that of a pilot in the Active Set by this margin. The access network shall set this field to the threshold Candidate Set pilot to Active Set pilot ratio, in units of 0.5 dB. The access terminal shall support all the valid values specified by this field.

PilotDropTimer Timer value after which an action is taken by the access terminal for a pilot that is a member of the Active Set or Candidate Set, and whose strength has not become greater than the value specified by PilotDrop. If the pilot is a member of the Active Set, a RouteUpdate message is sent in the Connected State. If the pilot is a member of the Candidate Set, it will be moved to the Neighbor Set. The access network shall set this field to the drop timer value shown in Table 6.6.6.5.1-1 corresponding to the pilot drop timer value to be used by access terminals. The access terminal shall support all the valid values specified by this field.

DynamicThresholds This field shall be set to '1' if the following three fields are included in this record. Otherwise, this field shall be set to '0'.

SoftSlope This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to an unsigned binary number, which is used by the access terminal in the inequality criterion for adding a pilot to the Active Set or dropping a pilot from the Active Set. The access terminal shall support all the valid values specified by this field.

AddIntercept This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to a 2's complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.

DropIntercept This field shall be included only if DynamicThresholds is set to '1'. This field shall be set to a 2's complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.

NeighborMaxAge The access network shall set this field to the maximum AGE value beyond which the access terminal is to drop members from the Neighbor Set. The access terminal shall support all the valid values specified by this field.

Reserved The access network shall set this field to zero. The access terminal shall ignore this field. The length of this field shall be such that the entire record is octet-aligned.

6.6.6.5.2 ConfigurationResponse

The access terminal sends the ConfigurationResponse message to select one of the complex attributes offered by the access network. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The access terminal shall set the MessageID field of this message to 0x51.

If the access terminal is sending an attribute with the message, the access terminal shall set the ValueID field associated with this attribute to the ValueID field of the complex attribute the access terminal is accepting.

Channels	AC	RTC
Addressing		unicast

SLP	Best Effort
Priority	60

6.6.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{RUPType}$	Type field for this protocol	Table 2.3.6-1
$N_{RUPDefault}$	Subtype field for this protocol	0x0000
$N_{RUPActive}$	Maximum size of the Active Set	6
$N_{RUPCandidate}$	Maximum size of the Candidate Set	6
$N_{RUPNeighbor}$	Minimum size of the Neighbor Set	20
$T_{RUPPilotSupervision}$	Pilot supervision timer	10 seconds
$T_{RUPConnectionSetup}$	Maximum time to receive an indication at the AT that the connection is set up from the instant it receives a TrafficChannelAssignment message.	1 second

6.6.8 Interface to Other Protocols

6.6.8.1 Commands Sent

This protocol sends the following commands:

- ***ReverseTrafficChannelMAC.Activate***

- *ReverseTrafficChannelMAC.Deactivate*
- *ForwardTrafficChannelMAC.Activate*
- *ForwardTrafficChannelMAC.Deactivate*

6.6.8.2 Indications

This protocol registers to receive the following indications:

- *ReverseTrafficChannelMAC.LinkAcquired*
- *OverheadMessages.Updated*

6.7 Default Packet Consolidation Protocol

6.7.1 Overview

The Default Packet Consolidation Protocol provides packet consolidation on the transmit side and provides packet de-multiplexing on the receive side. Packet consolidation is provided between different streams at the access terminal and between different streams associated with one access terminal, as well as between different access terminals at the access network.

6.7.2 Primitives and Public Data

6.7.2.1 Commands

This protocol does not define any commands.

6.7.2.2 Return Indications

This protocol does not return any indications.

6.7.2.3 Public Data

- None

6.7.3 Basic Protocol Numbers

The Type field for the Packet Consolidation Protocol is one octet, set to $N_{PCPType}$.

The Subtype field for the Default Packet Consolidation Protocol is two octets, set to $N_{PCPDefault}$.

6.7.4 Protocol Data Unit

The Protocol Data Unit for this protocol is a Connection Layer packet. Connection Layer packets contain Session Layer packets destined to or from the same access terminal address.

Two types of Connection Layer packets are defined:

- Format A: These packets are maximum length packets (including lower layer headers). Format A packets contain one Session Layer packet and do not have Connection Layer headers or padding.
- Format B: These packets are maximum length packets (including lower layer headers). Format B packets contain one or more Session Layer packets and have a Connection Layer header(s). The protocol places the Connection Layer header defined in 6.7.6.2 in front of each Session Layer packet and enough padding to create a maximum length packet.

Format A provides an extra byte of payload per packet.

The packet format type is passed with the packet to the lower layers.

The Connection Layer encapsulation is shown in Figure 6.7.4-1 and Figure 6.7.4-2.

All transmitted packets are forwarded to the Security Layer.

All received packets are forwarded to the Session Layer after removing the Connection Layer headers.

The maximum size Session Layer packet the protocol can encapsulate depends on the Physical Layer channel on which this packet will be transmitted and on the specific security protocols negotiated.

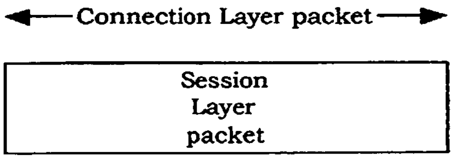


Figure 6.7.4-1. Connection Layer Packet Structure (Format A)

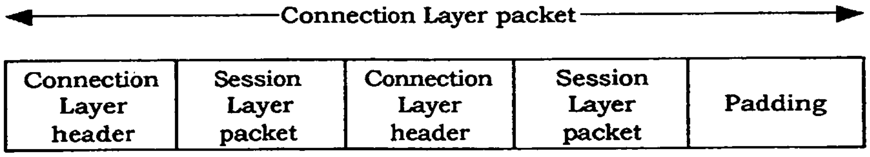


Figure 6.7.4-2. Connection Layer Packet Structure (Format B)

6.7.5 Procedures

This protocol does not have any initial configuration requirements.

This protocol receives the following information with every transmitted Session Layer packet:

- Destination channel: Forward Traffic Channel, Control Channel, Reverse Traffic Channel, or Access Channel.
- Priority.
- Forced Single Encapsulation: Whether or not the Session Layer packet can be encapsulated with other Session Layer packets in the same Connection Layer packet.

6.7.5.1 Destination Channels

If the destination channel is the Forward Traffic Channel, the packet also carries a parameter indicating whether the protocol is allowed to transmit it in a Control Channel capsule.

If the destination channel is the Control Channel, the packet also carries a parameter indicating whether the packet must be transmitted in a synchronous capsule. If the packet does not have to be transmitted in a synchronous capsule, it may carry a parameter indicating a transmission deadline.

6.7.5.2 Priority Order

Packets are prioritized according to the following rules:

- If two packets have different priority numbers, the packet with the lower priority number has priority.
- If two packets have the same priority number, the packet that was received first by the protocol has priority.

Transmission of packets that have higher priority shall take precedence over transmission of packets with lower priority.

Processing packets that have higher priority shall take precedence over processing packets with lower priority.

6.7.5.3 Forced Single Encapsulation

If a Forward Traffic Channel Session Layer packet is marked as Forced Single Encapsulation, the access network shall encapsulate it without any other Session Layer packets in a Connection Layer packet. The Packet Consolidation Protocol shall also pass an indication down to the physical layer with the Connection Layer packet, instructing the physical layer to ensure that the Physical Layer packet containing this packet does not contain any other Connection Layer packet. Forced Single Encapsulation applies only to the Forward Traffic Channel MAC Layer packets.

Forced Single Encapsulation is used for test services that require a one to one mapping between application packets and Physical Layer packets.

6.7.5.4 Access Terminal Procedures

6.7.5.4.1 Format A Packets

The access terminal shall create a Format A Connection Layer packet, only if the highest priority pending Session Layer packet will fill the Security Layer payload.

The access terminal shall forward the Connection Layer packet for transmission to the Security Layer.

6.7.5.4.2 Format B Packets

The access terminal shall create a Format B Connection Layer packet by adding the Connection Layer header, defined in 6.7.6.2 in front of every Session Layer packet, concatenating the result and adding enough padding to fill the Security Layer payload. The resulting packet length shall not exceed the maximum payload that can be carried on the Physical Layer Channel, given the transmission rate that will be used to transmit the packet and the headers added by the lower layers. All concatenated Connection Layer packets shall be transmitted on the same Physical Layer Channel.[29]

The protocol shall encapsulate and concatenate Session Layer packets in priority order.

The access terminal shall forward the Connection Layer packet for transmission to the Security Layer.

6.7.5.5 Access Network Procedures

6.7.5.5.1 Control Channel

The Control Channel carries broadcast transmissions as well as directed transmissions to multiple access terminals.

If the access network transmits a unicast packet to an access terminal over the Control Channel, it should transmit this packet at least from all the sectors in the access terminal's Active Set. If the data is carried in a synchronous capsule, the transmission should occur simultaneously at least once.

The access network shall create the Connection Layer packets as defined in 6.7.5.5.1.1.

The access network shall prioritize Connection Layer packets marked for transmission in a Control Channel synchronous capsule as defined in 6.7.5.5.1.2.

The access network shall prioritize Connection Layer packets marked for transmission in a Control Channel asynchronous capsule as defined in 6.7.5.5.1.1 and 6.7.5.5.1.3

6.7.5.5.1.1 Control Channel Connection Layer Packets

The access network shall not encapsulate Session Layer packets destined to different access terminals in the same Connection Layer packet.

The access network may encapsulate multiple Session Layer packets destined to a single access terminal in the same Connection Layer packet.

The access network should assign a priority to the Connection Layer packet based on its component Session Layer packets. If the Connection Layer packet contains a single Session Layer packet, the priority of the Connection Layer packet should be the priority received with the Session Layer packet.

If any Session Layer packet encapsulated in a Connection Layer packet is marked for transmission in a synchronous capsule, the Connection Layer packet shall be marked for transmission in a synchronous capsule.

The access network shall create a Connection Layer packet by appending the Connection Layer header defined in 6.7.6.2 in front of every Session Layer packet it is encapsulating in this Connection Layer packet and then concatenating the result. The resulting packet

[29] i.e., Access Channel or Reverse Traffic Channel.

length shall not exceed the maximum payload that can be carried in a Control Channel MAC Layer packet given the headers added by the lower layers.

The access network shall forward the Connection Layer packet for transmission to the Security Layer.

6.7.5.5.1.2 Synchronous Capsule Priority Rules

The access network should transmit, in priority order, all Connection Layer packets marked for transmission in a Control Channel synchronous capsule. If the amount of transmitted data (including lower layer headers) exceeds a single Control Channel MAC Layer packet, the access network may extend the synchronous capsule, delay the transmission of some Session Layer packets, or discard Session Layer packets. If the access network discards packets, it should discard them in reverse priority order.

In addition to transmitting the above Connection Layer packets, the access network may also transmit the following packets in a synchronous Control Channel capsule:

- Packets marked for transmission in an asynchronous Control Channel capsule, in priority order
- Packets marked for transmission either on the Forward Traffic Channel or the Control Channel, in priority order

If the access network transmits these additional packets, it should follow the above priority ordering, and should transmit them at a lower priority than packets marked for transmission in synchronous capsules only.

6.7.5.5.1.3 Asynchronous Capsule Priority Rules

Transmitting asynchronous capsules on the Control Channel is optional, because all data marked for transmission in these capsules can also be transmitted in a synchronous capsule.

If the access network chooses to transmit Connection Layer packets in an asynchronous capsule of the Control Channel, it should do so in the following order:

- Packets marked for transmission in an asynchronous capsule of the Control Channel, in priority order
- Packets marked for transmission either on the Forward Traffic Channel or the Control Channel, in priority order

6.7.5.5.2 Forward Traffic Channel

The Forward Traffic Channel is time-multiplexed between the different access terminals. The transmission priority given to each access terminal is beyond the scope of this specification.[30]

[30] Typical considerations for the access network are throughput maximization balanced with a fairness criteria between users.

6.7.5.5.2.1 Format A Packets

The access network shall create a Format A Connection Layer packet, only if the length of the highest priority pending Session Layer packet will fill the security layer payload.

The access network shall forward the Connection Layer packet for transmission to the Security Layer.

6.7.5.5.2.2 Format B Packets

The access network shall create a Format B Connection Layer packet by adding the Connection Layer header defined in 6.7.6.2 in front of every Session Layer packet, concatenating the result and adding padding to fill the Security Layer payload. The resulting packet length shall not exceed the maximum payload that can be carried on the Forward Traffic Channel given the headers added by the lower layers.

The protocol shall encapsulate and concatenate Session Layer packets in priority order.

The access network shall forward the Connection Layer packet for transmission to the Security Layer.

6.7.6 Header Format

6.7.6.1 Pad

The access network shall add sufficient padding so that the packet fills the Security Layer payload.

The access network shall set the padding bits to '0'. The access terminal shall ignore the padding bits.

6.7.6.2 Connection Layer Header

The access terminal and the access network add the following header in front of every Session Layer packet encapsulated in a Format B Connection Layer packet.

Field	Length (bits)
Length	8

Length Length of Session Layer packet in octets.

6.7.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{PCPType}$	Type field for this protocol	Table 2.3.6-1
$N_{PCPDefault}$	Subtype field for this protocol	0x0000

6.7.8 Interface to Other Protocols

6.7.8.1 Commands Sent

This protocol does not issue any commands.

6.7.8.2 Indications

This protocol does not register to receive any indications.

6.8 Overhead Messages Protocol

6.8.1 Overview

The QuickConfig message and the SectorParameters message are collectively termed the overhead messages. These messages are broadcast by the access network over the Control Channel. These messages are unique, in that they pertain to multiple protocols and are, therefore, specified separately. The Overhead Messages Protocol provides procedures related to transmission, reception and supervision of these messages.

This protocol can be in one of two states:

- Inactive State: In this state, the protocol waits for an ***Activate*** command. This state corresponds only to the access terminal and occurs when the access terminal has not acquired an access network or is not required to receive overhead messages.
- Active State: In this state the access network transmits and the access terminal receives overhead messages.

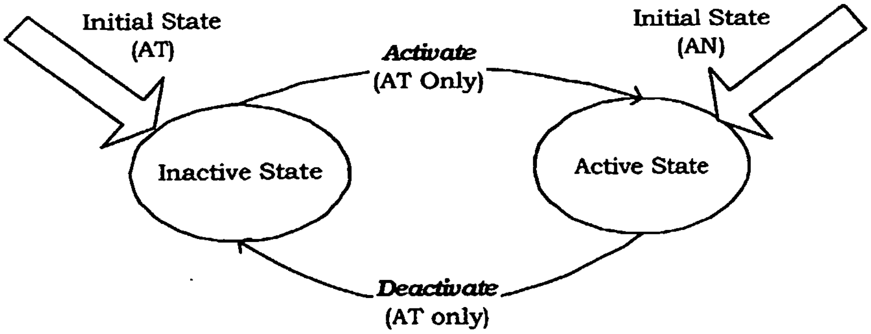


Figure 6.8.1-1. Overhead Messages Protocol State Diagram

6.8.2 Primitives and Public Data

6.8.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***

6.8.2.2 Return Indications

This protocol returns the following indications:

- ***ANRedirected***
- ***SupervisionFailed***
- ***Updated***

6.8.2.3 Public Data

This protocol shall make the following data public:

- all data in the overhead messages
- OverheadParametersUpToDate

6.8.3 Basic Protocol Numbers

The Type field for the Overhead Messages is one octet, set to $N_{OMPType}$.

The Subtype field for this protocol is two octets set to $N_{OMPDefault}$.[31]

6.8.4 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol; and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

6.8.5 Procedures

6.8.5.1 Protocol Initialization and Configuration

The access terminal shall start this protocol in the Inactive State.

The access network shall start this protocol in the Active State.

This protocol does not have any initial configuration requirements.

6.8.5.2 Extensibility Requirements

Further revisions of the access network may add new overhead messages.

The access terminal shall discard overhead messages with a MessageID field it does not recognize.

Further revisions of the access network may add new fields to existing overhead messages. These fields shall be added to the end of the message, prior to the Reserved field if such a field is defined.

The access terminal shall ignore fields it does not recognize.

6.8.5.3 Command Processing

The access network shall ignore all commands.

6.8.5.3.1 Activate

If this protocol receives an ***Activate*** command in the Inactive State:

- The access terminal shall transition to the Active State.

[31] This protocol is not negotiable; and, therefore, the protocol Subtype is currently not used.

- The access network shall ignore it.

If this protocol receives the command in the Active State, it shall be ignored.

6.8.5.3.2 Deactivate

If this protocol receives a ***Deactivate*** command in the Inactive State, it shall be ignored.

If this protocol receives the command in the Active State:

- Access terminal shall transition to the Inactive State.
- Access network shall ignore it.

6.8.5.4 Access Network Requirements

The access network shall include a QuickConfig message in every Control Channel synchronous capsule. The access network should include a SectorParameters message in the synchronous capsule at least once every $N_{OMPSectorParameters}$ Control Channel cycles. The access network shall set the SectorSignature field of the QuickConfig message to the SectorSignature field of the next SectorParameters message. The access network shall set the AccessSignature field of the QuickConfig message to the public data AccessSignature (see Default Access Channel MAC Protocol).

6.8.5.5 Access Terminal Requirements

When the access terminal is required to keep the overhead messages updated, it shall perform supervision on the QuickConfig and the SectorParameters messages as specified in 6.8.5.5.1.1 and 6.8.5.5.1.2, respectively.

If the access terminal does not have any stored value for the overhead parameters or if it receives a ***RouteUpdate.IdleHO*** indication, the access terminal shall set OverheadParametersUpToDate to 0.

When the access terminal receives the QuickConfig message, it shall perform the following:

- If the value of the SectorSignature field of the new QuickConfig message is different from the stored value for SectorSignature, the access terminal shall perform the following:
  - The access terminal shall set OverheadParametersUpToDate to 0.
  - The access terminal shall monitor every subsequent Control Channel synchronous capsule until it receives the updated SectorParameters message. When the access terminal receives the updated SectorParameters message, it shall return an ***Updated*** indication and set OverheadParametersUpToDate to 1.
- Otherwise, the access terminal shall perform the following:
  - The access terminal shall set OverheadParametersUpToDate to 1.
  - The access terminal shall return an ***Updated*** indication.

Once the access terminal receives an updated overhead message, it should store the signature associated with the message for future comparisons. The access terminal may cache overhead message parameters and signatures to speed up acquisition of parameters from a sector that was previously monitored.

If the Redirect field of the QuickConfig message is set to '1', the access terminal shall return an ***ANRedirected*** indication.[32]

6.8.5.5.1 Supervision Procedures

6.8.5.5.1.1 Supervision of QuickConfig Message

Upon entering the Active State, the access terminal shall start the following procedure to supervise the QuickConfig message:

- The access terminal shall set a QuickConfig supervision timer for $T_{OMPQCSupervision}$.
- If a QuickConfig message is received while the timer is active, the access terminal shall reset and restart the timer.
- If the timer expires, the access terminal shall return a ***SupervisionFailed*** indication and disable the timer.

6.8.5.5.1.2 Supervision of SectorParameters Message

Upon entering the Active State, the access terminal shall start the following procedure to supervise the SectorParameters message:

- The access terminal shall set a SectorParameters supervision timer for $T_{OMPSPSupervision}$.
- If a SectorParameters message is received while the timer is active, the access terminal shall reset and restart the timer.
- If the timer expires, the access terminal shall return a ***SupervisionFailed*** indication and disable the timer.

6.8.6 Message Formats

6.8.6.1 QuickConfig

The QuickConfig message is used to indicate a change in the overhead messages' contents and to provide frequently changing information.

[32] Redirection is commonly used in networks under test.

Field	Length (bits)
MessageID	8
ColorCode	8
SectorID24	24
SectorSignature	16
AccessSignature	16
Redirect	1
RPCCount	6

RPCCount occurrences of the following field

DRCLock	1

RPCCount occurrences of the following field

ForwardTrafficValid	1

Reserved	variable

MessageID The access network shall set this field to 0x00.

ColorCode The access network shall set this field to he color code corresponding to this sector.

SectorID24 The access network shall set this field to the least significant 24 bits of the SectorID value corresponding to this sector.

SectorSignature The access network shall set this field to the value of the SectorSignature field of the next SectorParameters message it will transmit.

AccessSignature The access network shall set this field to the value of the AccessSignature parameter from the AccessParameters message that is Public Data of the Access Channel MAC Protocol.

Redirect Access network redirect. The access network shall set this field to '1' if it is redirecting all access terminals away from this access network.[33]

[33] Network redirect is commonly used during testing.

RPCCount The access network shall set this field to the maximum number of RPC channels supported by the sector.

DRCLock The access network shall set occurrence ***n*** of this field to '1' if it has received a valid DRC from the access terminal that has been assigned MACIndex 64-***n*** (e.g., occurrence 1 of this field, corresponds to MACIndex 63).

ForwardTrafficValid The access network shall set occurrence ***n*** of this field to '1' if the Forward Traffic Channel associated with MACIndex 64-***n*** is valid. The access terminal uses this field to perform supervision of the Forward Traffic Channel.

Reserved The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CCsyn
Addressing	broadcast

SLP	Best Effort
Priority	10

6.8.6.2 SectorParameters

The SectorParameters message is used to convey sector specific information to the access terminals.

Field	Length (bits)
MessageID	8
SectorID	128
SubnetMask	8
SectorSignature	16
Latitude	22
Longitude	23
RouteUpdateRadius	11
LeapSeconds	8
LocalTimeOffset	11
ChannelCount	5

ChannelCount occurrences of the following field:

Channel	24

NeighborCount	5

NeighborCount occurrences of the following field:

NeighborPilotPN	9

NeighborCount occurrences of the following two fields:

NeighborChannelIncluded	1
NeighborChannel	0 or 24

NeighborSearchWindowSizeIncluded	1

NeighborCount occurences of the following field

NeighborSearchWindowSize	0 or 4

NeighborSearchWindowOffsetIncluded	1

NieghborCount occurrences of the following field

NieghborSearchWindowOffset	0 or 3

Field	Length (bits)
Reserved	Variable

MessageID The access network shall set this field to 0x01.

SectorID Sector Address Identifier. The access network shall set this field to the 128-bit address of this sector.

SubnetMask Sector Subnet identifier. The access network shall set this field to the number of consecutive 1's in the subnet mask of the subnet to which this sector belongs.

SectorSignature SectorParameters message signature. The access network shall change this field if the contents of the SectorParameters message changes.

Latitude The latitude of the sector. The access network shall set this field to this sector's latitude in units of 0.25 second, expressed as a two's complement signed number with positive numbers signifying North latitudes. The access network shall set this field to a value in the range -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°).

Longitude The longitude of the sector. The access network shall set this field to this sector's longitude in units of 0.25 second, expressed as a two's complement signed number with positive numbers signifying East longitude. The access network shall set this field to a value in the range -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°).

RouteUpdateRadius If access terminals are to perform distance based route updates, the access network shall set this field to the non-zero "distance" beyond which the access terminal is to send a new RouteUpdate message (see Default Route Update Protocol). If access terminals are not to perform distance based route updates, the access network shall set this field to 0.[34]

LeapSeconds The number of leap seconds that have occurred since the start of system time.

[34] The access terminal determines whether to send a distance based RouteUpdate message or not using the RouteUpdateRadius value of the serving sector. If the serving sector allows distance based Route Updates, the access terminal uses the RouteUpdateRadius value sent by the sector in which the access terminal last registered.

LocalTimeOffset

The access network shall set this field to the offset of the local time from System Time. This value will be in units of minutes, expressed as a two's complement signed number.

ChannelCount

The access network shall set this field to the number of cdma2000 high rate packet data channels available to the access terminal on this sector.

Channel

Channel record specification for each channel. See 10.1 for the Channel record format. The access network shall set the SystemType field of this record to 0x00.

NeighborCount

The access network shall set this field to the number of records specifying neighboring sectors information included in this message.

NeighborPilotPN

The access network shall set this field to the PN Offset of neighboring sector that the access terminal should add to its Neighbor Set.

NeighborChannelIncluded

The access network shall set this field to '1' if a Channel record is included for this neighbor, and to '0' otherwise. The *n*th occurrence of this field corresponds to the *n*th occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.

NeighborChannel

Channel record specification for the neighbor channel. See 10.1 for the Channel record format. The access network shall omit this field if the corresponding NeighborChannelIncluded field is set to '0'. Otherwise, if included, the *n*th occurrence of this field corresponds to the *n*th occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.

NeighborSearchWindowSizeIncluded

The access network shall set this field to '1' if NeighborSeachWindowSize field for neighboring sectors is included in this message. Otherwise, the access network shall set this field to '0'.

NeighborSearchWindowSize

The access network shall omit this field if NieghborSearchWindowSizeIncluded is set to '0'. If NeighborSearchWindowSizeIncluded is set to '1', the acess network shall set this field to the value shown in Table 6.8.6.2-1 corresponding to the search window size to be used by the access terminal for the neighbor pilot. The *n*th occurrence of this field corresponds to the n^{th} occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.

Table 6.8.6.2-1. Search Window Sizes

SearchWindowSize Value	Search Window Size (PN chips)
0	4
1	6
2	8
3	10
4	14
5	20
6	28
7	40
8	60
9	80
10	100
11	130
12	160
13	226
14	320
15	452

NeighborSearchWindowOffsetIncluded

The access network shall set this field to '1' if NeighborSeachWindowOffset field for neighboring sectors is included in this message. Otherwise, the access network shall set this field to '0'.

NeighborSeachWindowOffset

The access network shall omit this field if NeighborSearchWindowOffsetIncluded is set to '0'. If NeighborSearchWindowOffsetIncluded is set to '1', the acess network shall set this field to the value shown in Table 6.8.6.2-2 corresponding to the search window offset to be used by the access terminal for the neighbor pilot. The n^{th} occurrence of this field corresponds to the *n*th occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.

Table 6.8.6.2-2. Search Window Offset

SearchWindowOffset	Offset (PN chips)
0	0
1	WindowSize[35] /2
2	WindowSize
3	3 × WindowSize /2
4	- WindowSize /2
5	- WindowSize
6	-3 × WindowSize /2
7	Reserved

Reserved The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC	SLP	Best Effort
Addressing	broadcast	Priority	30

6.8.7 Protocol Numeric Constants

Constant	Meaning	Value

[35] WindowSize is pilot's search window size in PN chips.

Constant	Meaning	Value
$N_{OMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{OMPDefault}$	Subtype field for this protocol	0x0000
$T_{OMPQCSupervision}$	QuickConfig supervision timer	12 Control Channel cycles
$T_{OMPSPSupervision}$	SectorParameters supervision timer	12 Control Channel cycles
$N_{OMPSectorParameters}$	The recommended maximum number of Control Channel cycles between two consecutive SectorParameters message transmissions	3

6.8.8 Interface to Other Protocols

6.8.8.1 Commands Sent

This protocol does not send any commands.

6.8.8.2 Indications

This protocol registers to receive the following indication:

- ***RouteUpdate.IdleHO***

No text.

7 SECURITY LAYER

7.1 Introduction

7.1.1 General Overview

The Security Layer provides the following functions:

- Key Exchange: Provides the procedures followed by the access network and by the access terminal to exchange security keys for authentication and encryption.
- Authentication: Provides the procedures followed by the access network and the access terminal for authenticating traffic.
- Encryption: Provides the procedures followed by the access network and the access terminal for encrypting traffic.

The Security Layer uses the Key Exchange Protocol, Authentication Protocol, Encryption Protocol, and Security Protocol to provide these functions. Security Protocol provides public variables needed by the authentication and encryption protocols (e.g., cryptosync, time-stamp, etc.).

Figure 7.1.1-1 shows the protocols within the Security Layer.

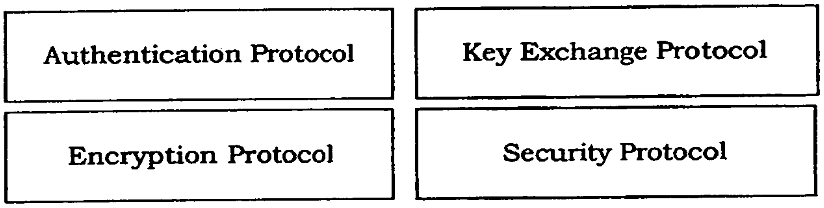


Figure 7.1.1-1. Security Layer Protocols

7.2 Data Encapsulation

Figure 7.2-1 illustrates the relationship between a Connection Layer packet, a Security Layer packet and a MAC Layer payload.

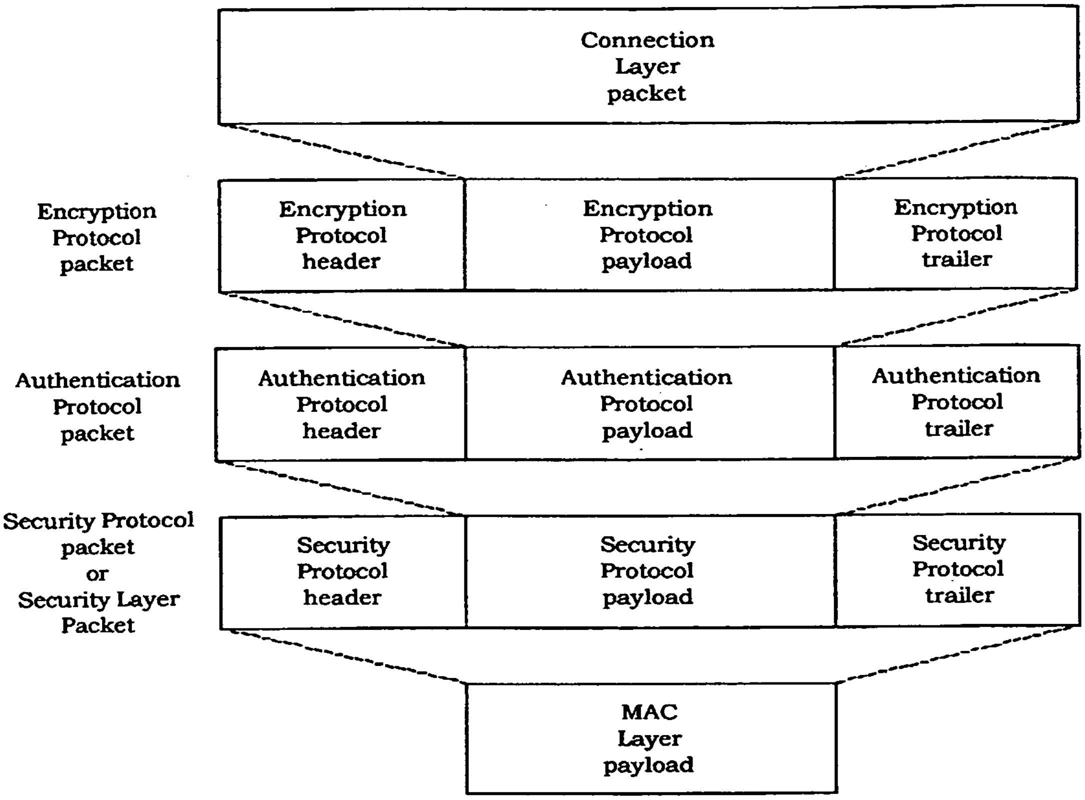

Connection Layer packet
Encryption Protocol packet
Encryption Protocol header
Encryption Protocol payload
Encryption Protocol trailer
Authentication Protocol packet
Authentication Protocol header
Authentication Protocol payload
Authentication Protocol trailer
Security Protocol packet or Security Layer Packet
Security Protocol header
Security Protocol payload
Security Protocol trailer
MAC Layer payload

Figure 7.2-1. Security Layer Encapsulation

The Security Layer headers or trailers may not be present (or equivalently, have a size of zero) if session configuration establishes the Default Security Layer or if the configured Security Protocol does not require a header or trailer. The fields added by the MAC Layer indicate presence (or absence) of the Security Layer headers and trailers. The Encryption Protocol may add a trailer to hide the actual length of the plain-text or padding to be used by the encryption algorithm. The Encryption Protocol Header may contain variables such as initialization vector (IV) to be used by the Encryption Protocol. The Authentication Protocol header or trailer may contain the digital signature that is used to authenticate the portion of the Authentication Protocol Packet that is authenticated. The Security Protocol header or trailer may contain variables needed by the authentication and encryption protocols (e.g., cryptosync, time-stamp, etc.).

Figure 7.2-1 shows the portions of the security layer packet that may be encrypted and authenticated. The authentication is performed on the Encryption Protocol Packet. This avoids unnecessary decryption when authentication fails.

The Security Layer shall pass the ConnectionLayerFormat field given to it by the MAC Layer to the Connection Layer with the Connection Layer packet.

7.2.1 Primitives and Public Data

7.2.1.1 Key Exchange Protocol

7.2.1.1.1 Commands

This protocol does not define any commands.

7.2.1.1.2 Return Indications

This protocol does not return any indication.

7.2.1.1.3 Public Data

- FACAuthKey
  The authentication key for use on Forward Assigned Channels (e.g., the Forward Traffic Channel).
- RACAuthKey
  The authentication key for use on Reverse Assigned Channels (e.g., the Reverse Traffic Channel).
- FACEncKey
  The encryption key for use on Forward Assigned Channels (e.g., the Forward Traffic Channel).
- RACEncKey
  The encryption key for use on Reverse Assigned Channels (e.g., the Reverse Traffic Channel).
- FPCAuthKey
  The authentication key for use on Forward Public Channels (e.g., the Control Channel).
- RPCAuthKey
  The authentication key for use on Reverse Public Channels (e.g., the Access Channel).
- FPCEncKey
  The encryption key for use on Forward Public Channels (e.g. the Control Channel).
- RPCEncKey
  The encryption key for use on Reverse Public Channels (e.g. the Access Channel).

7.2.1.1.4 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{KEPType}$.

7.2.1.1.5 Interface to Other Protocols

7.2.1.1.5.1 Commands

This protocol does not define any commands.

7.2.1.1.5.2 Indications

This protocol does not register to receive any indications.

7.2.1.2 Encryption Protocol

7.2.1.2.1 Commands

This protocol does not define any commands.

7.2.1.2.2 Return Indications

This protocol returns the following indication:

- ***Failed***

7.2.1.2.3 Public Data

This protocol does not define any public data.

7.2.1.2.4 Basic Protocol Numbers

The Type field for this protocol is one octet, set to N_{EPType}.

7.2.1.2.5 Interface to Other Protocols

7.2.1.2.5.1 Commands

This protocol does not issue any commands.

7.2.1.2.5.2 Indications

This protocol does not register to receive any indications.

7.2.1.3 Authentication Protocol

7.2.1.3.1 Commands

This protocol does not define any commands.

7.2.1.3.2 Return Indications

This protocol returns the following indication:

- ***Failed***

7.2.1.3.3 Public Data

This protocol does not define any public data.

7.2.1.3.4 Basic Protocol Numbers

The Type field for this protocol is one octet, set to N_{APType}.

7.2.1.3.5 Interface to Other Protocols

7.2.1.3.5.1 Commands

This protocol does not issue any commands.

7.2.1.3.5.2 Indications

This protocol does not register to receive any indications.

7.2.1.4 Security Protocol

7.2.1.4.1 Commands

This protocol does not define any commands.

7.2.1.4.2 Return Indications

This protocol does not return any indications.

7.2.1.4.3 Public Data

- TimeStampLong

7.2.1.4.4 Basic Protocol Numbers

The Type field for this protocol is one octet, set to N_{SPType}.

7.2.1.4.5 Interface to Other Protocols

7.2.1.4.5.1 Commands

This protocol does not issue any commands.

7.2.1.4.5.2 Indications

This protocol does not register to receive any indications.

7.3 Default Security Protocol

7.3.1 Overview

The Default Security Protocol does not provide any services, except for transferring packets between the Authentication Protocol and the MAC layer.

7.3.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to $N_{SPDefault}$.

7.3.3 Protocol Data Unit

The protocol data unit for this protocol is a Security Layer packet. Each Security Layer packet consists of an Authentication Protocol packet.

The protocol shall set the Security Layer packet to the Authentication Protocol packet and shall forward it for transmission to the MAC Layer. This protocol does not define a Security Protocol header or trailer.

This protocol shall set the Authentication Protocol packet to the Security Layer packet received from the MAC Layer, and shall forward the packet to the Authentication Protocol.

7.3.4 Default Security Protocol Header

The Default Security Protocol does not add a header.

7.3.5 Default Security Protocol Trailer

The Default Security Protocol does not add a trailer.

7.3.6 Protocol Numeric Constants

Constant	Meaning	Value
N_{SPType}	Type field for this protocol	Table 2.3.6-1
$N_{SPDefault}$	Subtype field for this protocol	0x0000

7.4 Generic Security Protocol

7.4.1 Overview

The Generic Security protocol performs the following tasks:

- On the transmission side, this protocol provides a Time Stamp that may be used by the negotiated Authentication Protocol and Encryption Protocol.
- On the receiving side, this protocol computes the Time Stamp using the information provided in the Security Protocol header and makes the Time Stamp publicly available.

7.4.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to $N_{SPGeneric}$.

7.4.3 Protocol Data Unit

The protocol data unit for this protocol is a Security Layer packet. Each Security Layer packet consists of an Authentication Protocol packet and a Security Protocol header.

The protocol shall construct a Security Layer packet out of the Authentication Protocol packet as follows and shall pass the packets for transmission to the MAC Layer:

- When the protocol receives an Authentication Protocol packet from the Authentication Protocol that is either authenticated or encrypted, it shall set TimeStampShort in the Security protocol header to the least significant 16 bits of the value of the TimeStampLong that is used by the Authentication Protocol or the Encryption Protocol to authenticate or encrypt this packet. The Security Protocol shall then add the Security Protocol header in front of the Authentication Protocol packet. The packet structure is shown in Figure 7.2-1.
- When the protocol receives an Authentication Protocol packet from the Authentication Protocol that is neither authenticated nor encrypted, the protocol shall not add a security protocol header to the Authentication Protocol packet.
- This protocol shall not append a Security Protocol trailer to the Authentication Protocol packet.

This Security Protocol shall construct the Authentication Protocol packet using the Security Layer packet (received from the MAC Layer) as follows and shall forward the packet to the Authentication Protocol:

- When the protocol receives a Security Layer packet from the MAC Layer that is either authenticated or encrypted, it shall construct the Authentication Protocol packet by removing the Security Layer header.
- When the protocol receives a Security Layer packet from the MAC Layer that is neither authenticated nor encrypted, it shall set the Authentication Protocol packet to the Security Layer packet.

7.4.4 Procedures

When the Security Layer receives a Connection Layer packet that is to be either authenticated or encrypted, the Security Protocol shall choose a value for the TimeStampLong based on the current 64-bit representation of the CDMA System Time in units of 80 ms, such that TimeStampLong does not specify a time later than the time that the security layer packet will be transmitted by the physical layer, and is not earlier than the current CDMA System Time[36]. The protocol shall then set TimeStampShort in the Security Protocol header to TimeStampLong[15:0].

When the Security Protocol receives a Security Layer packet from the MAC Layer that is either authenticated or encrypted, it shall compute the 64-bit TimeStampLong using TimeStampShort given in the Security Protocol Header as follows:

$$\text{TimeStampLong} = (\text{SystemTime} - (\text{SystemTime}[15:0] - \text{TimeStampShort}) \bmod 2^{16}) \bmod 2^{64},$$

where SystemTime is the current CDMA System Time in units of 80 ms, SystemTime[15:0] is the 16 least significant bits of the SystemTime, and TimeStampShort is the 16-bit Security protocol header.

7.4.5 Generic Security Protocol Header

The Generic Security Protocol Header is as follows:

Field	Length(bits)
TimeStampShort	0 or 16

TimeStampShort — The sender shall include this field, only if the Authentication Protocol packet is either authenticated or encrypted. The sender shall set this field to the 16 least significant bits of the TimeStampLong.

7.4.6 Generic Security Protocol Trailer

The Generic Security Protocol does not add a trailer.

7.4.7 Protocol Numeric Constants

Constant	Meaning	Value
N_{SPType}	Type field for this protocol	Table 2.3.6-1
$N_{SPGeneric}$	Subtype field for this protocol	0x0001

[36] For example, the protocol may choose the current CDMA System Time as TimeStampLong.

7.5 Default Key Exchange Protocol

7.5.1 Overview

The Default Key Exchange Protocol does not provide any services and is selected when the Default Authentication Protocol and the Null encryption Protocol are selected.

7.5.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets and is set to $N_{KEPDefault}$.

7.5.2.1 Initialization

The protocol in the access terminal and access network shall set all of the following variables to NULL:

- SKey
- FACAuthKey
- RACAuthKey
- FACEncKey
- RACEncKey
- FPCAuthKey
- RPCAuthKey
- FPCEncKey
- RPCEncKey

7.5.3 Protocol Data Unit

This protocol does not carry payload on behalf of other layers or protocols.

7.5.4 Protocol Numeric Constants

Constant	Meaning	Value
$N_{KEPType}$	Type field for this protocol	Table 2.3.6-1
$N_{KEPDefault}$	Subtype field for this protocol	0x0000

7.6 DH Key Exchange Protocol

7.6.1 Overview

The DH Key Exchange Protocol provides a method for session key exchange based on Diffie-Hellman (DH).

7.6.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets and is set to N_{KEPDH}.

7.6.3 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

7.6.4 Procedures

The Key Exchange Protocol uses the KeyRequest and KeyResponse messages for exchanging public session keys, and the ANKeyComplete and ATKeyComplete messages for indicating that the secret session keys have been calculated.

The access terminal and the access network shall perform the following key exchange procedure during session configuration.

7.6.4.1 Initialization

The protocol in the access terminal and access network shall initialize all the following variables to NULL:

- SKey
- FACAuthKey
- RACAuthKey
- FACEncKey
- RACEncKey
- FPCAuthKey
- RPCAuthKey
- FPCEncKey
- RPCEncKey

7.6.4.2 Access Network Requirements

The access network shall initiate the key exchange by sending a KeyRequest message. The access network shall choose a random number ANRand between KeyLength and $2^{KeyLength} - 2$ and set the ANPubKey field of the KeyRequest message as follows:

$$\text{ANPubKey} = g^{\text{ANRand}} \bmod p$$

where g, p, and KeyLength are specified during session configuration of the DH Key Exchange Protocol.

The random number ANRand should have the following properties:

- The number generated should have a uniform statistical distribution over its range.
- The numbers used in formulating different KeyRequest messages should be statistically uncorrelated.
- The number used in formulating each KeyRequest message should not be derivable from the previously used random numbers.
- The numbers used in formulating KeyRequest message sent by different access networks should be statistically uncorrelated.

If the access network does not receive a KeyResponse message with a TransactionID field that matches the TransactionID field of the associated KeyRequest message, within $T_{KEPANResponse}$, the access network shall declare failure and stop performing the rest of the key exchange procedure.

After receiving a KeyResponse message with a TransactionID field that matches the TransactionID field of the associated KeyRequest message, the access network shall perform the following:

- The access network shall set $T_{KEPKeyCompAT}$ to the duration of time specified by Timeout, reported by the access terminal in the KeyResponse message. The access network shall then start the AT Key Computation Timer with a time-out value of $T_{KEPKeyCompAT}$.
- The access network shall compute SKey, the session key as follows:

  $$\text{SKey} = \text{ATPubKey}^{\text{ANRand}} \bmod p$$

- The access network shall construct the ***message bits,*** as shown in Table 7.6.4.2-1, using the computed SKey, TimeStampLong, the TransactionID, and a 16-bit pseudo-random value, Nonce. TimeStampLong is a 64-bit value that is set, based on the current 64-bit representation of the CDMA System Time in units of 80 ms, such that TimeStampLong does not specify a time later than the time that the message will be transmitted by physical layer and is not earlier than the current CDMA System Time[37].

[37] For example, the protocol may choose the current CDMA System Time as TimeStampLong.

Table 7.6.4.2-1. Message Bits

Field	Length(bits)
SKey	KeyLength
TransactionID	8
Nonce	16
TimeStampLong	64

- The access network shall pad the ***message bits*** constructed in the previous step, as specified in [6], and compute the 160-bit ***message digest*** as specified in [6].
- The access network shall send an ANKeyComplete message with the KeySignature field of the message set to the ***message digest*** computed in the previous step and the TimeStampShort field of the message set to the 16 least significant bits of the CDMA System Time used in the previous step. The access network shall then start the AT Signature Computation Timer with a time-out value of $T_{KEPSigCompAN}$.

The access network shall disable both the AT Key Computation Timer and the AT Key Signature Computation Timer when it receives an ATKeyComplete message with a TransactionID that matches the TransactionID field of the associated KeyRequest and KeyResponse messages.

The access network shall declare failure and stop performing the rest of the key exchange procedure if any of the following events occur:

- Both AT Key Computation and the AT Key Signature Computation Timers are expired, or
- Access network receives an ATKeyComplete message with Result field set to '0'.

7.6.4.3 Access Terminal Requirements

Upon receiving the KeyRequest message, the access terminal shall perform the following:

- The access terminal shall choose a random number ATRand between KeyLength and $2^{KeyLength}$ –2 and set the ATPubKey field of the KeyResponse message as follows:

  ATPubKey = g^{ATRand} mod p

  where g and p are KeyLength dependent protocol constants for the DH Key Exchange protocol, and KeyLength is specified during session configuration of the DH Key Exchange Protocol.

- The access terminal shall send a KeyResponse message with the ATPubKey field set to the value computed in the previous step, within $T_{KEPATResponse}$ second of receiving a KeyRequest message.
- The access terminal shall compute SKey, the session key as follows:

  SKey = ANPubKey ^{ATRand} mod p.

The random number ATRand should have the following properties:

- Number generated should have a uniform statistical distribution over its range,
- Numbers used in formulating different KeyResponse messages should be statistically uncorrelated,
- Number used in formulating each KeyResponse message should not be derivable from the previously used random numbers,
- Numbers used in formulating KeyResponse message sent by different access terminals should be statistically uncorrelated.

After the access terminal sends a KeyResponse message, it shall set $T_{KEPKeyCompAN}$ to the duration of time specified by Timeout, reported by the access network in the KeyRequest message. The access terminal shall then start the AN Key Computation Timer with a time-out value of $T_{KEPKeyCompAN}$. The access terminal shall disable the AN Key Computation Timer when it receives the ANKeyComplete message with a TransactionID that matches the TransactionID field of the associated KeyRequest and KeyResponse messages.

When the AN Key Computation Timer expires, the access terminal shall declare failure.

After receiving an ANKeyComplete message with a TransactionID field that matches the TransactionID field of the associated KeyRequest message, the access terminal shall perform the following:

- Access terminal shall compute the 64-bit variable TimeStampLong as follows:

  TimeStampLong = (SystemTime – (SystemTime[15:0] – TimeStampShort) mod 2^{16}) mod 2^{64},

  where SystemTime is the current CDMA System Time in units of 80 ms, SystemTime[15:0] is the 16 least significant bits of the SystemTime, and TimeStampShort is the 16-bit field received in the ANKeyComplete message.

- Access terminal shall construct the ***message bits*** as shown in Table 7.6.4.3-1 using the computed SKey, computed TimeStampLong, and TransactionID, and Nonce fields of the ANKeyComplete message.

Table 7.6.4.3-1. Message Bits

Field	Length(bits)
Skey	KeyLength
TransactionID	8
Nonce	16
TimeStampLong	64

- Access terminal shall pad the ***message bits*** constructed in the previous step, as specified in [6], and compute the 160-bit ***message digest*** as specified in [6].

- If the ***message digest*** computed in the previous step matches the KeySignature field of ANKeyComplete message, the access terminal shall send an ATKeyComplete message with the Result field set to '1' within $T_{KEPSigCompAT}$ seconds of the latter of the following two events:
  - Reception of the ANKeyComplete message.
  - Finishing computing the SKey.
- Otherwise, the access terminal shall declare failure and send an ATKeyComplete message with the Result field set to '0'.

7.6.4.4 Authentication Key and Encryption Key Generation

The keys used for authentication and encryption are generated from the session key, SKey, using the procedures specified in this section.

Table 7.6.4.4-1 defines eight sub-fields within the SKey. These sub-fields are of equal length.

Table 7.6.4.4-1. Subfields of SKey

Sub-Field	Length (bits)
K0	KeyLength / 8
K1	KeyLength / 8
K2	KeyLength / 8
K3	KeyLength / 8
K4	KeyLength / 8
K5	KeyLength / 8
K6	KeyLength / 8
K7	KeyLength / 8

The access network and access terminal shall construct the ***message bits*** as shown in Figure 7.6.4.4-1. In this figure, TimeStampLong and Nonce are the same as the one used for generation of KeySignature (see 7.6.4.2, and 7.6.4.3).

	MSB		LSB
Message bits for generation of FACAuthKey	K0 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of RACAuthKey	K1 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of FACEncKey	K2 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of RACEncKey	K3 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of FPCAuthKey	K4 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of RPCAuthKey	K5 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of FPCEncKey	K6 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
Message bits for generation of RPCEncKey	K7 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)

Figure 7.6.4.4-1. Message Bits for Generation of Authentication and Encryption Keys

The access terminal and access network shall then pad the ***message bits*** constructed in the previous step, as specified in [6], and compute the 160-bit ***message digests*** (for each of the eight keys) as specified in [6]. The access network and access terminal shall set the FACAuthKey, RACAuthKey, FACEncKey, RACEncKey, FPCAuthKey, RPCAuthKey, FPCEncKey, and RPCEncKey to the ***message digests*** for the corresponding key as shown in Figure 7.6.4.4-1.

7.6.5 Message Formats

7.6.5.1 KeyRequest

The access network sends the KeyRequest message to initiate the session key exchange.

Field	Length (bits)
MessageID	8
TransactionID	8
Timeout	8
ANPubKey	KeyLength (as negotiated)

MessageID The access network shall set this field to 0x00.

TransactionID The access network shall increment this value for each new KeyRequest message sent.

Timeout Shared secret calculation timeout. The access network shall set this field to the maximum time in the number of seconds that the access network requires for calculation of the session key (SKey).

ANPubKey Access network's ephemeral public Diffie-Hellman key. The access network shall set this field to the ephemeral public Diffie-Hellman key of the access network as specified in 7.6.4.2.

Channels	CC	FTC
Addressing		unicast

SLP	Reliable
Priority	40

7.6.5.2 KeyResponse

The access terminal sends the KeyResponse message in response to the KeyRequest message.

Field	Length (bits)
MessageID	8
TransactionID	8
Timeout	8
ATPubKey	KeyLength (as negotiated)

MessageID The access terminal shall set this field to 0x01.

TransactionID — The access terminal shall set this field to the value of the TransactionID field of the KeyRequest message to which the access terminal is responding.

Timeout — Shared secret calculation timeout. The access terminal shall set this field to the maximum time in seconds that the access terminal requires for calculation of the session key (SKey).

ATPubKey — Access terminal's ephemeral public Diffie-Hellman key. The access terminal shall set this field to the ephemeral public Diffie-Hellman key of the access terminal as specified in 7.6.4.3.

Channels	RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.6.5.3 ANKeyComplete

The access network sends the ANKeyComplete message in response to the KeyResponse message.

Field	Length (bits)
MessageID	8
TransactionID	8
Nonce	16
TimeStampShort	16
KeySignature	160

MessageID — The access network shall set this field to 0x02.

TransactionID — The access network shall set this field to the value of the TransactionID field of the corresponding KeyRequest message.

Nonce — The access network shall set this field to an arbitrarily chosen 16-bit value Nonce that is used to compute the KeySignature.

TimeStampShort — The access network shall set this field to the 16 least significant bits of the SystemTimeLong used in computing the KeySignature as specified in 7.6.4.2.

KeySignature — The access network shall set this field to the 20-octet signature of the session key (SKey) as specified in 7.6.4.2.

Channels	CC FTC	SLP	Reliable
Addressing	unicast	Priority	40

7.6.5.4 ATKeyComplete

The access terminal sends the ATKeyComplete message in response to the ANKeyComplete message.

Field	Length (bits)
MessageID	8
TransactionID	8
Result	1
Reserved	7

MessageID The access terminal shall set this field to 0x03.

TransactionID The access terminal shall set this field to the value of the TransactionID field of the corresponding KeyRequest message.

Result The access terminal shall set this field to '1' if the KeySignature field of ANKeyComplete message matches the ***message digest*** computed for the KeySignature as specified in 7.6.4.3; otherwise the access terminal shall set this field to '0'.

Reserved The access terminal shall set this field to zero. The access network shall ignore this field.

Channels	RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.6.5.5 Configuration Messages

The DH Key Exchange Protocol uses the Generic Configuration Protocol for configuration. All configuration messages sent by this protocol shall have their Type field set to $N_{KEPType}$.

Unless stated otherwise, all attributes are simple attributes.

The configurable attributes for this protocol are listed in Table 7.6.5.5-1.

The access terminal shall use as defaults the values Table 7.6.5.5-1 typed in *bold italics*.

Table 7.6.5.5-1. Configurable Values

Attribute ID	Attribute	Values	Meaning
0x00	Session Key Length (KeyLength)	0x00	Default is 96-octet (768-bit) Diffie-Hellman key. KeyLength = 768
		0x01	128-octet (1024-bit) Diffie-Hellman key. KeyLength = 1024
		0x02-0xff	Reserved

7.6.5.5.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for the Key Exchange Protocol. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.6.5.5.2 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.6.6 Protocol Numeric Constants

Constant	Meaning	Value
$N_{KEPType}$	Type field for this protocol	Table 2.3.6-1
N_{KEPDH}	Subtype field for this protocol	0x0001
$T_{KEPSigCompAN}$	Time to receive ATKeyComplete after sending ANKeyComplete	3.5 seconds
$T_{KEPSigCompAT}$	Time to send ATKeyComplete after receiving ANKeyComplete	3 seconds
$T_{KEPANResponse}$	Time to receive KeyResponse after sending KeyRequest	3.5 seconds
$T_{KEPATResponse}$	Time to send KeyResponse after receiving KeyRequest	3 second

Table 7.6.5.5-1. Common Primitive Base and Common Prime Modulus for KeyLength equal to 768[38]

Constant	Meaning	Value		
g	Common primitive base	0x02		
p	Common prime modulus (MSB first)	0xFFFFFFFF	0xFFFFFFFF	0xC90FDAA2
		0x2168C234	0xC4C6628B	0x80DC1CD1
		0x29024E08	0x8A67CC74	0x020BBEA6
		0x3B139B22	0x514A0879	0x8E3404DD
		0xEF9519B3	0xCD3A431B	0x302B0A6D
		0xF25F1437	0x4FE1356D	0x6D51C245
		0xE485B576	0x625E7EC6	0xF44C42E9
		0xA63A3620	0xFFFFFFFF	0xFFFFFFFF

Table 7.6.5.5-2. Common Primitive Base and Common Prime Modulus for KeyLength equal to 1024

Constant	Meaning	Value		
g	Common primitive base	0x02		
p	Common prime modulus (MSB first)	0xFFFFFFFF	0xFFFFFFFF	0xC90FDAA2
		0x2168C234	0xC4C6628B	0x80DC1CD1
		0x29024E08	0x8A67CC74	0x020BBEA6
		0x3B139B22	0x514A0879	0x8E3404DD
		0xEF9519B3	0xCD3A431B	0x302B0A6D
		0xF25F1437	0x4FE1356D	0x6D51C245
		0xE485B576	0x625E7EC6	0xF44C42E9
		0xA637ED6B	0x0BFF5CB6	0xF406B7ED
		0xEE386BFB	0x5A899FA5	0xAE9F2411
		0x7C4B1FE6	0x49286651	0xECE65381
		0xFFFFFFFF	0xFFFFFFFF	

7.6.7 Message Flows

Figure 7.6.7-1 shows an example flow diagram in which the access network quickly computes the Key and the signature and sends it to the access terminal. The access terminal still needs time to finish the Key calculation. In this case the ***AT Signature Computation Timer*** expires, but the ***AT Key Computation Timer*** does not expire.

[38] The values for p and g are taken from [7].

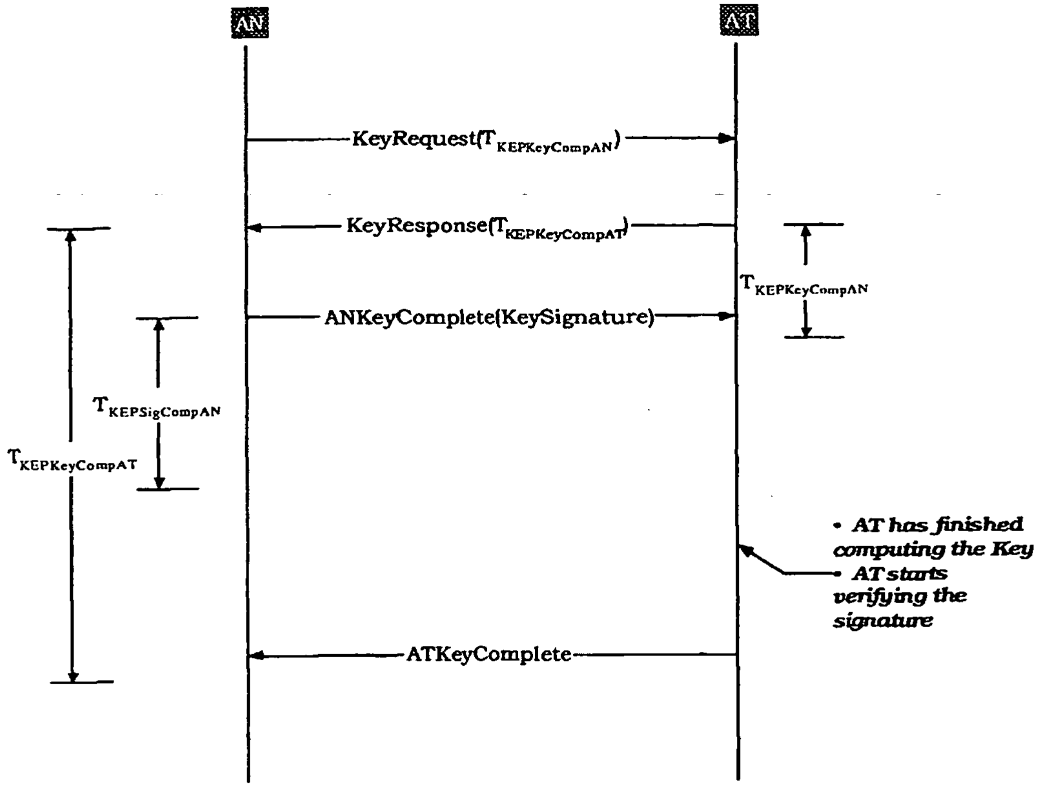

AN
AT
KeyRequest($T_{KEPKeyCompAN}$)
KeyResponse($T_{KEPKeyCompAT}$)
ANKeyComplete(KeySignature)
ATKeyComplete
$T_{KEPKeyCompAN}$
$T_{KEPSigCompAN}$
$T_{KEPKeyCompAT}$
• AT has finished computing the Key
• AT starts verifying the signature

Figure 7.6.7-1. Example Call Flow: Timer $T_{KEPSigCompAN}$ Expires But $T_{KEPKeyCompAT}$ Does Not Expire

Figure 7.6.7-2 shows an example flow diagram in which the access network requires a longer period of time to compute the Key. In this case the ***AT Key Computation Timer*** expires, but the ***AT Signature Computation Timer*** does not expire.

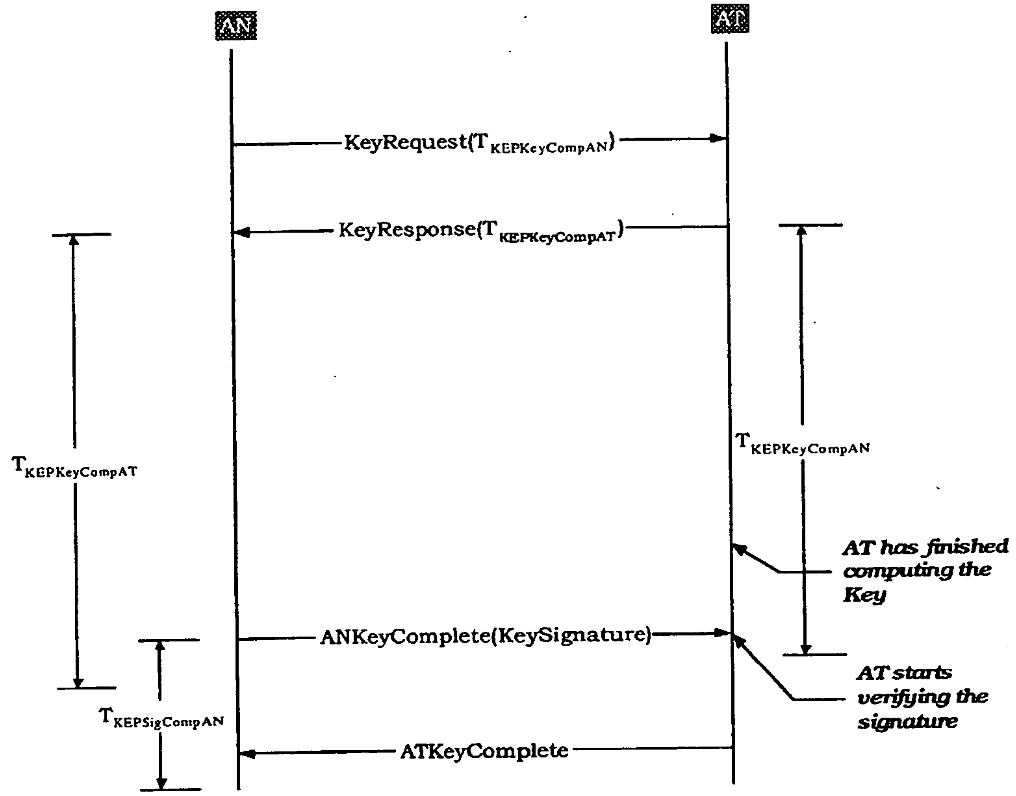

AN
AT
KeyRequest($T_{KEPKeyCompAN}$)
KeyResponse($T_{KEPKeyCompAT}$)
$T_{KEPKeyCompAT}$
$T_{KEPKeyCompAN}$
AT has finished computing the Key
ANKeyComplete(KeySignature)
AT starts verifying the signature
$T_{KEPSigCompAN}$
ATKeyComplete

Figure 7.6.7-2. Example Call Flow: Timer $T_{KEPSigCompAN}$ Does Not Expire But $T_{KEPKeyCompAT}$ Expires

7.7 Default Authentication Protocol

7.7.1 Overview

The Default Authentication Protocol does not provide any services except for transferring packets between the Encryption Protocol and the Security Protocol.

7.7.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to $N_{APDefault}$.

7.7.3 Protocol Data Unit

The protocol data unit for this protocol is an Authentication Protocol packet.

When this protocol receives Encryption Protocol packets, it shall forward them to the Security Protocol.

When the protocol receives a Security Protocol packet from the Security Protocol, it shall set the Encryption Protocol packet to the Authentication Protocol packet and shall forward the Encryption Protocol packet to the Encryption Protocol.

7.7.4 Default Authentication Protocol Header

The Default Authentication Protocol does not add a header.

7.7.5 Default Authentication Protocol Trailer

The Default Authentication Protocol does not add a trailer.

7.7.6 Protocol Numeric Constants

Constant	Meaning	Value
N_{APType}	Type field for this protocol	Table 2.3.6-1
$N_{APDefault}$	Subtype field for this protocol	0x0000

7.8 SHA-1 Authentication Protocol

7.8.1 Overview

The SHA-1 Authentication Protocol provides a method for authentication of the Access Channel MAC Layer packets by applying the SHA-1 hash function to ***message bits*** that are composed of the ACAuthKey, security layer payload, CDMA System Time, and the sector ID.

7.8.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to N_{APSHA1}.

7.8.3 Protocol Data Unit

The protocol data unit for this protocol is an Authentication Protocol packet. This protocol receives Encryption Protocol Packets and adds the authentication layer header defined in 7.8.5 in front of each Access Channel Encryption Protocol Packet to make an Access Channel Authentication Protocol Packet and forwards it to the Security protocol.

When the protocol receives Access Channel Security protocol packets from the Security protocol, it constructs the Encryption Protocol Packet by removing the Authentication Protocol Header, and forwards the Encryption Protocol Packet to the Encryption Protocol.

7.8.4 Procedures

The procedures in 7.8.4.1 and 7.8.4.2 shall apply to packets carried by the Access Channel. For all other packets, the Default Authentication Protocol defined in 7.7 shall apply.

7.8.4.1 Access Network Requirements

Upon reception of an Authentication Protocol packet from the Access Channel, the access network shall compute and verify the Access Channel MAC Layer packet authentication code (ACPAC) given in the authentication protocol header as follows:

- The access network shall construct the ACAuthKey from the RPCAuthKey public data of the Key Exchange Protocol as follows:
  - If the length of RPCAuthKey is equal to the length of ACAuthKey, then ACAuthKey shall be RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is greater than the length of ACAuthKey, then ACAuthKey shall be the ACAuthKeyLengh least significant bits of RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is less than the length of ACAuthKey, then ACAuthKey shall be set to RPCAuthKey with zeros concatenated to the end (LSB) of it, such that the length of the result is ACAuthKeyLength.
- The access network shall construct the ***message bits*** for computing ACPAC as shown in Table 7.8.4.1-1:

Table 7.8.4.1-1. Message Bits for ACPAC Computation

Field	Length(bits)
ACAuthKey	ACAuthKeyLength
Authentication Protocol Payload	variable
SectorID	128
TimeStampLong	64

where SectorID is provided as public data by the Overhead Messages protocol and TimeStampLong is the 64-bit public value provided by the Security layer protocol.

- The access network shall pad the ***message bits*** constructed in the previous step, as specified in [6], and compute the 160-bit ***message digest*** as specified in [6] and set ACPAC to the 64 least significant bits of the ***message digest***.

If the ACPAC computed in the previous step matches the ACPAC field in the Protocol Header, then the Protocol shall deliver the Authentication Layer Payload to the Encryption Protocol. Otherwise, the Protocol shall issue a ***Failed*** indication and shall discard the security layer packet.

7.8.4.2 Access Terminal Requirements

Upon reception of an Encryption Protocol packet destined for the Access Channel, the access terminal shall compute ACPAC as follows:

- The access terminal shall construct the ACAuthKey from the RPCAuthKey public data of the Key Exchange Protocol as follows:
  - If the length of RPCAuthKey is equal to the length of ACAuthKey, then ACAuthKey shall be RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is greater than the length of ACAuthKey, then ACAuthKey shall be the ACAuthKeyLengh least significant bits of RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is less than the length of ACAuthKey, then ACAuthKey shall be the concatination of zeros at the end (LSB) of RPCAuthKey, such that the length of the result is ACAuthKeyLength.
- The access terminal shall construct the ***message bits*** for computing ACPAC as shown in Table 7.8.4.2-1:

Table 7.8.4.2-1. Message Bits for ACPAC Computation

Field	Length(bits)
ACAuthKey	ACAuthKeyLength
Authentication Protocol Payload	variable
SectorID	128
TimeStampLong	64

where SectorID is provided as public data by the Overhead Messages Protocol and TimeStampLong is the 64-bit public value provided by the Security Protocol.

- The access terminal shall pad the ***message bits*** constructed in the previous step, as specified in [6], and compute the 160-bit ***message digest*** as specified in [6] and set the ACPAC field to the 64 least significant bits of the ***message digest***.

7.8.5 SHA-1 Authentication Protocol Header Format

The SHA-1 Authentication Protocol is as follows:

Field	Length(bits)
ACPAC	64

ACPAC Access Channel Packet Authentication Code. The access terminal shall compute this field as specified in 7.8.4.2.

7.8.6 SHA-1 Authentication Protocol Trailer

The SHA-1 Authentication Protocol does not add a trailer.

7.8.6.1 Configuration Messages

The SHA-1 Authentication Protocol uses the Generic Configuration Protocol for configuration. All configuration messages sent by this protocol shall have their Type field set to N_{APType}.

Unless stated otherwise, all attributes are simple attributes.

The configurable attributes for this protocol are listed in Table 7.8.6.1-1.

The access terminal shall use as defaults the values Table 7.8.6.1-1 typed in *bold italics*.

Table 7.8.6.1-1. Configurable Values

Attribute ID	Attribute	Values	Meaning
0x00	ACAuthKeyLength	*0x00A0*	Default value for the authentication key length in bits.
		0x0000 – 0xFFFF	Access Channel authentication key length in bits.

7.8.6.1.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to request the configuration of one or more parameters for the Authentication Protocol. The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x50.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.8.6.1.2 ConfigurationResponse

The sender sends the ConfigurationResponse message to select one of the parameter settings offered in an associated ConfigurationRequest message. The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The sender shall set the MessageID field of this message to 0x51.

Channels	FTC RTC	SLP	Reliable
Addressing	unicast	Priority	40

7.8.7 Protocol Numeric Constants

Constant	Meaning	Value
N_{APType}	Type field for this protocol	Table 2.3.6-1
N_{APSHA1}	Subtype field for this protocol	0x0001

7.9 Default Encryption Protocol

The Default Encryption Protocol does not alter the Security Layer packet payload (i.e., no encryption/decryption) and does not add an Encryption Protocol Header or Trailer; therefore, the Cipher-text for this protocol is equal to the Connection Layer packet. If needed, end-to-end encryption can be provided at the application layer (which is outside the scope of this specification).

7.9.1 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to $N_{EPDefault}$.

7.9.2 Protocol Data Unit

The protocol data unit for this protocol is an Encryption Protocol Packet. The Encryption Protocol Packet for this protocol is the same as the Connection Layer packet.

7.9.3 Default Encryption Protocol Header

The Default Encryption Protocol does not add a header.

7.9.4 Default Encryption Protocol Trailer

The Default Encryption Protocol does not add a trailer.

7.9.5 Protocol Numeric Constants

Constant	Meaning	Value
N_{EPType}	Type field for this protocol	Table 2.3.6-1
$N_{EPDefault}$	Subtype field for this protocol	0x0000

No text.

8 MAC LAYER

8.1 Introduction

8.1.1 General Overview

The MAC Layer contains the rules governing operation of the Control Channel, Access Channel, Forward Traffic Channel, and Reverse Traffic Channel.

This section presents the default protocols for the MAC Layer. Each of these protocols can be independently negotiated at the beginning of the session.

The MAC Layer contains the following protocols:

- Control Channel MAC Protocol: This protocol builds Control Channel MAC Layer packets out of one or more Security Layer packets, contains the rules concerning access network transmission and packet scheduling on the Control Channel, access terminal acquisition of the Control Channel, and access terminal Control Channel MAC Layer packet reception. This protocol also adds the access terminal address to transmitted packets.
- Access Channel MAC Protocol: This protocol contains the rules governing access terminal transmission timing and power characteristics for the Access Channel.
- Forward Traffic Channel MAC Protocol: This protocol contains the rules governing operation of the Forward Traffic Channel. It dictates the rules the access terminal follows when transmitting the Data Rate Control Channel, along with the rules the access network uses to interpret this channel. The protocol supports both variable rate and fixed rate operation of the Forward Traffic Channel.
- Reverse Traffic Channel MAC Protocol: This protocol contains the rules governing operation of the Reverse Traffic Channel. It dictates the rules the access terminal follows to assist the access network in acquiring the Reverse Traffic Channel. It also dictates the rules the access terminal and the access network use to select the transmission rate used over the Reverse Traffic Channel.

The relationship between the MAC layer protocols is shown in Figure 8.1.1-1.

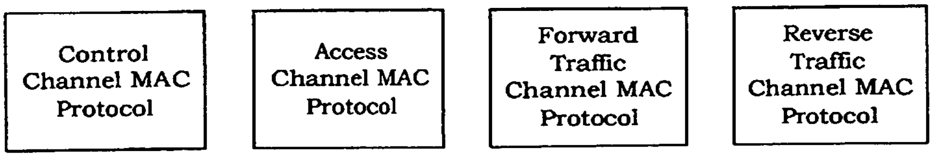

Control Channel MAC Protocol
Access Channel MAC Protocol
Forward Traffic Channel MAC Protocol
Reverse Traffic Channel MAC Protocol

Figure 8.1.1-1. MAC Layer Protocols

8.1.2 Data Encapsulation

In the transmit direction, the MAC Layer receives Security Layer packets, adds layer-related headers, trailers and padding, and forwards the resulting packet for transmission to the Physical Layer.

In the receive direction, the MAC Layer receives MAC packets from the Physical Layer and forwards them to the Security Layer after removing the layer-related headers, trailers and padding.

Figure 8.1.2-1, Figure 8.1.2-2, Figure 8.1.2-3, and Figure 8.1.2-4 illustrate the relationship between Security Layer packets, MAC packets and Physical Layer packets for the Control Channel, Access Channel, and the Forward and Reverse Traffic Channels.

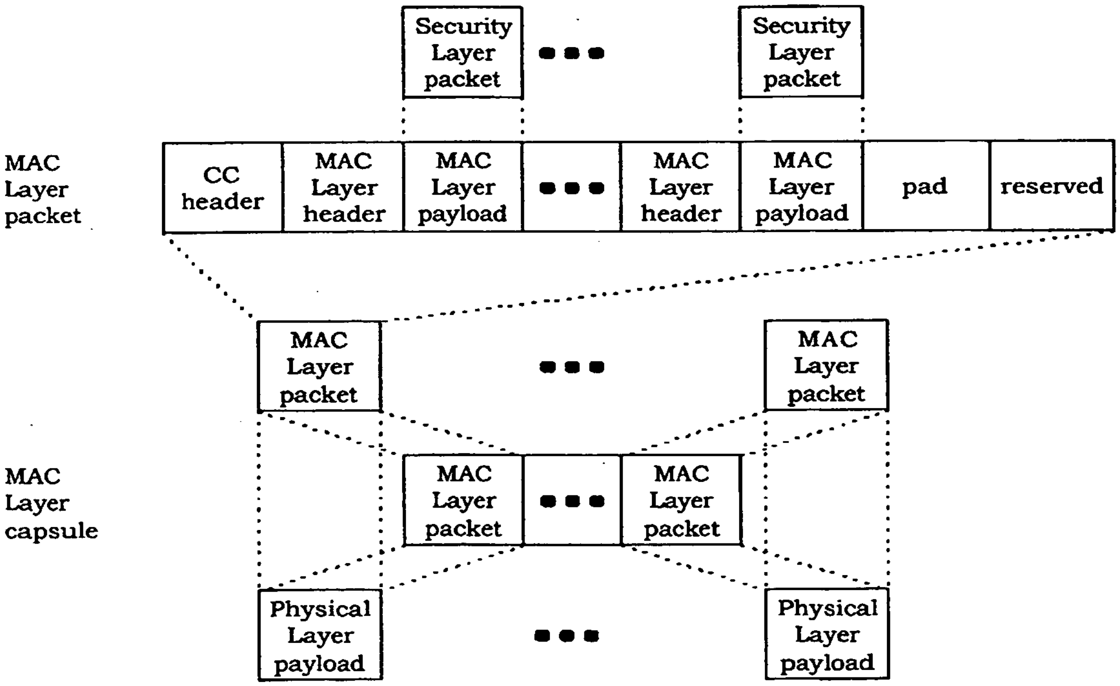


Figure 8.1.2-1. Control Channel MAC Layer Packet Encapsulation

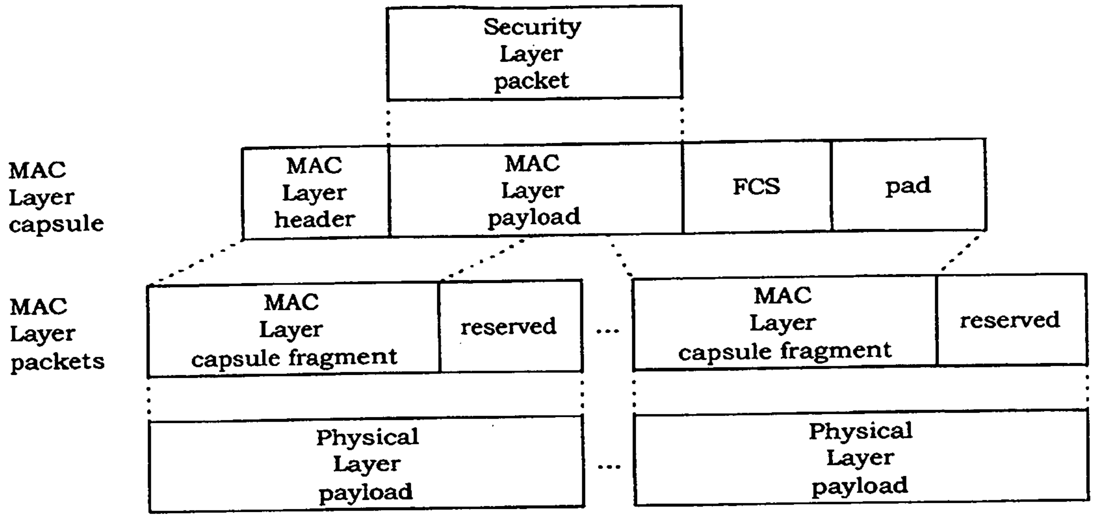


Figure 8.1.2-2. Access Channel MAC Layer Packet Encapsulation

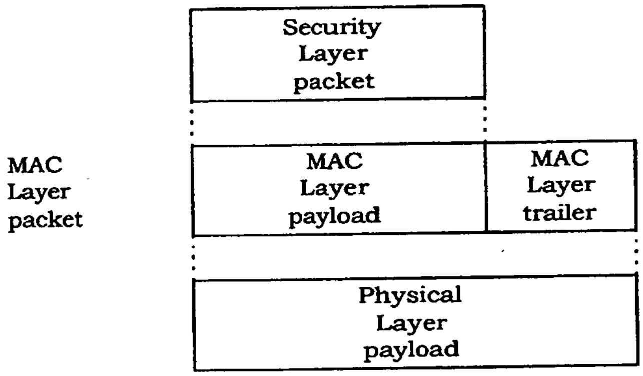


Figure 8.1.2-3. Forward Traffic Channel MAC Layer Packet Encapsulation

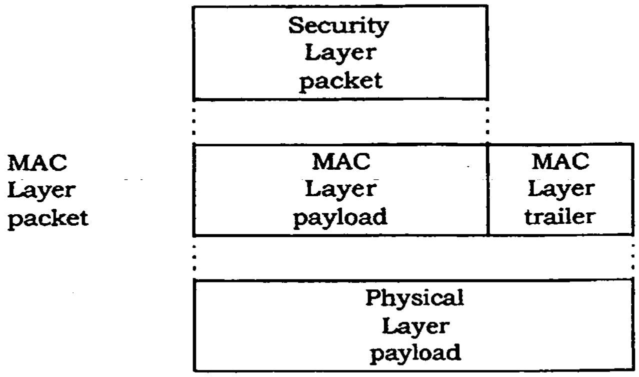


Figure 8.1.2-4. Reverse Traffic Channel MAC Layer Packet Encapsulation

8.2 Default Control Channel MAC Protocol

8.2.1 Overview

The Default Control Channel MAC Protocol provides the procedures and messages required for an access network to transmit and for an access terminal to receive the Control Channel.

This specification assumes that the access network has one instance of this protocol for all access terminals.

This protocol can be in one of two states:

- Inactive State: in this state the protocol waits for an ***Activate*** command. This state corresponds only to the access terminal and occurs when the access terminal has not acquired an access network or is not monitoring the Control Channel.
- Active State: in this state the access network transmits and the access terminal receives the Control Channel.

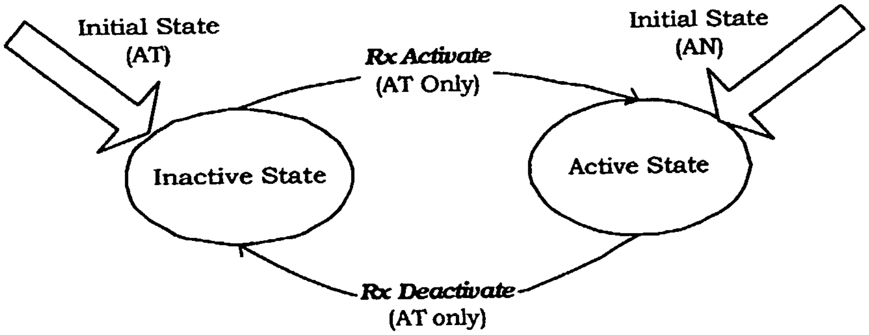


Figure 8.2.1-1. Default Control Channel MAC Protocol State Diagram

8.2.2 Primitives and Public Data

8.2.2.1 Commands

This protocol defines the following commands:

- ***Activate.***
- ***Deactivate.***

8.2.2.2 Return Indications

This protocol returns the following indications:

- ***SupervisionFailed***

8.2.2.3 Public Data

- None.

8.2.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{CCMPType}$.

The Subtype field for this protocol is two octets, set to $N_{CCMPDefault}$.

8.2.4 Protocol Data Unit

The transmission unit of this protocol is the Control Channel MAC Layer packet. Each Control Channel MAC Layer packet consists of zero or more Security Layer packets for zero or more access terminals.

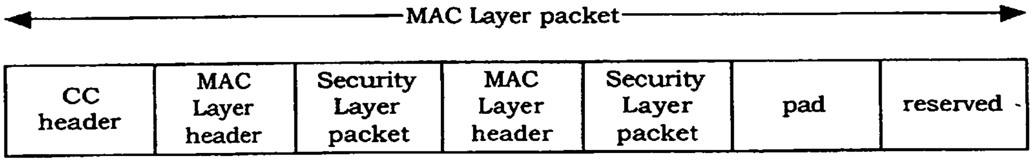
The protocol constructs a packet out of the Security Layer packets, as follows:

- It adds the MAC Layer header specified in 8.2.6.1 in front of every Security Layer packet.
- Concatenates the Control Channel Header specified in 8.2.6.2 followed by the above formed packets.
- Pads the resulting packet as defined in 8.2.6.3.
- Adds the reserved bits as defined in 8.2.6.4.

The protocol then sends the packet for transmission to the Physical Layer. The packet structure is shown in Figure 8.2.4-1.

Control Channel MAC Layer packets can be transmitted, either in a synchronous capsule, which is transmitted at a particular time, or in an asynchronous capsule which can be transmitted at any time, except when a synchronous capsule is transmitted. synchronous capsule consists of one or more Control Channel MAC Layer packets. An asynchronous capsule consists of one Control Channel MAC Layer packet.

This protocol expects an address and a parameter indicating transmission in synchronous or an asynchronous capsule with each transmitted Security Layer packet. For Security Layer packets that are carried by an asynchronous capsule, this protocol can also receive an optional parameter indicating a transmission deadline.



CC header	MAC Layer header	Security Layer packet	MAC Layer header	Security Layer packet	pad	reserved

Figure 8.2.4-1. Control Channel MAC Packet Structure

Received packets are parsed into their constituent Security Layer packets. The packets that are addressed to the access terminal (see 8.2.5.5.2.4) are then forwarded for further processing to the Security Layer.

8.2.5 Procedures

8.2.5.1 Protocol Initialization and Configuration

The access terminal shall start this protocol in the Inactive State.

The access network shall start this protocol in the Active State.

This protocol does not have any initial configuration requirements.

8.2.5.2 Command Processing

The access network shall ignore all commands.

8.2.5.2.1 Activate

If this protocol receives an ***Activate*** command in the Inactive State,

- The access terminal shall transition to the Active State
- The access network shall ignore it

If this protocol receives this command in the Active State it shall be ignored.

8.2.5.2.2 Deactivate

If this protocol receives a ***Deactivate*** command in the Inactive State, it shall be ignored.

If this protocol receives this command in the Active State,

- The access terminal shall transition to the Inactive State
- The access network shall ignore it

8.2.5.3 Control Channel Cycle

The Control Channel cycle is defined as a 256 slot period, synchronous with CDMA system time; i.e., there is an integer multiple of 256 slots between the beginning of a cycle and the beginning of CDMA system time.

8.2.5.4 Inactive State

This state applies only to the access terminal.

When the protocol is in the Inactive State, the access terminal waits for an ***Activate*** command.

8.2.5.5 Active State

In this state, the access network transmits, and the access terminal monitors the Control Channel.

8.2.5.5.1 Access Network Requirements

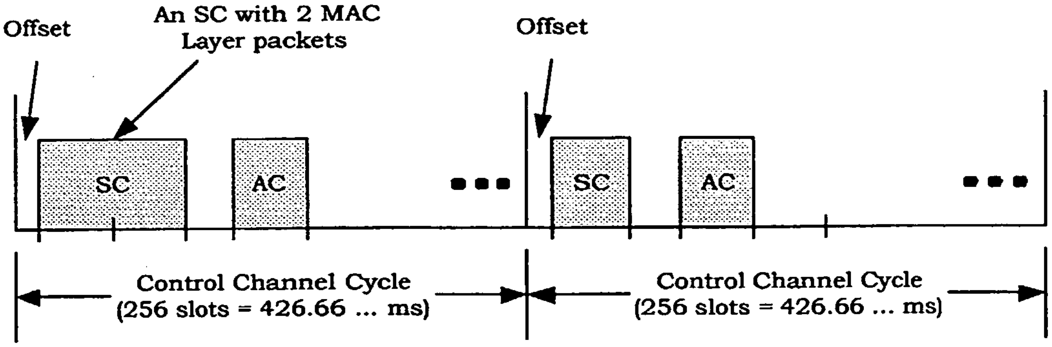
8.2.5.5.1.1 General Requirements

The access network shall always have one instance of this protocol operating per sector.

When the access network transmits the Control Channel, it shall do so using a rate of 38.4 kbps or 76.8 kbps.

The access network shall transmit synchronous capsules and it may transmit asynchronous capsules. When the access network transmits synchronous capsules, it shall comply with 8.2.5.5.1.2. When the access network transmits asynchronous capsules, it shall comply with 8.2.5.5.1.3.

The timing of synchronous and asynchronous capsules is shown in Figure 8.2.5.5.1.1-1.


Offset
An SC with 2 MAC Layer packets
Offset
SC
AC
SC
AC
Control Channel Cycle (256 slots = 426.66 ... ms)
Control Channel Cycle (256 slots = 426.66 ... ms)

SC: Synchronous Control Channel capsule.

AC: Asynchronous Control Channel capsule.

Figure 8.2.5.5.1.1-1. Location of Control Channel Capsules

8.2.5.5.1.2 Transmission of Synchronous Capsules

The access network shall construct a synchronous capsule out of all the pending Security Layer packets that are destined for transmission in a synchronous capsule. The synchronous capsule may contain more than one Control Channel MAC Layer packet.

The access network shall set the SynchronousCapsule bit of the Control Channel Header to '1' only for the first Control Channel MAC Layer packet of a synchronous capsule.

The access network shall set the LastPacket bit of the Control Channel Header to '1' only for the last Control Channel MAC Layer packet of a synchronous capsule.

The access network shall set the Offset field of the Control Channel Header to the same value for all the Control Channel MAC Layer packets of a synchronous capsule.

If the access network has no pending Security Layer packets, it shall transmit synchronous capsule with one Control Channel MAC Layer packet containing only the Control Channel header.The access network shall transmit the Control Channel MAC Layer packets of a synchronous capsule as follows:

- The first MAC Layer packet shall start transmission at times T where T satisfies the following equation:

  $T \bmod 256 = \text{Offset}.$

- All other MAC Layer packets of the capsule shall start transmission at the earliest time T following the end of transmission of the previous packet of the capsule that satisfies the following equation:

  $T \bmod 4 = \text{Offset},$

where T is CDMA System Time in slots and Offset is as specified in the Control Channel header of the packets.

8.2.5.5.1.3 Transmission of Asynchronous Capsules

The access network may transmit asynchronous capsules at any time during the Control Channel cycle in which it does not transmit a synchronous capsule. If the access network has queued Security Layer packets that are marked for transmission in an asynchronous capsule, it should transmit the packets no later than their associated transmission deadline, if one was provided. The access network may:

- Transmit these packets in a synchronous capsule.
- Transmit these packets in an asynchronous capsule.

The access network shall set the SynchronousCapsule bit of the Control Channel Header to '0' for the Control Channel MAC Layer packet of an asynchronous capsule.

The access network shall set the LastPacket bit of the Control Channel Header to '1' for the Control Channel MAC Layer packet of an asynchronous capsule.

The access network shall set the Offset field of the Control Channel Header to '00' for the Control Channel MAC Layer packet of an asynchronous capsule.

8.2.5.5.2 Access Terminal Requirements

8.2.5.5.2.1 Initial Acquisition

When the access terminal detects a Control Channel preamble and determines that the packet being transmitted is the first Control Channel MAC Layer packet of a synchronous capsule, it shall subtract Offset slots from the beginning of the half slot boundary at which the preamble was detected, and shall set the result to the beginning of the 16-slot frame and the beginning of the Control Channel Cycle.

8.2.5.5.2.2 Normal Operation

If the access terminal receives a Control Channel MAC Layer packet that has the LastPacket bit in the Control Channel header set to '0', the access terminal shall continue monitoring the Control Channel for the Control Channel MAC Layer packets of the same capsule until it either does not receive a Control Channel MAC Layer Packet at the designated timeor it receives a Control Channel MAC Layer packet with the LastPacket bit set to '1'.

8.2.5.5.2.3 Control Channel Supervision

Upon entering the active state, the access terminal shall set the Control Channel supervision timer for $T_{CCMPSupervision}$. If a Control Channel capsule is received while the timer is active, the timer is reset and restarted. If the timer expires the protocol returns a ***SupervisionFailed*** indication and disables the timer.

8.2.5.5.2.4 Address Matching

When the access terminal receives a Control Channel MAC packet, it shall perform the following:

- Access terminal shall parse the packet into its constituent Security Layer packets.
- Access terminal shall forward the Security Layer packet along with the SecurityLayerFormat and the ConnectionLayerFormat fields to the Security Layer if either of the following two conditions are met:
  - If the ATIType field and the ATI field of the ATI Record in the MAC Layer header of a Security Layer packet is equal to the ATIType and ATI fields of any member of the Address Management Protocol's ReceiveATIList.
  - If the ATIType of the ATI Record in the MAC Layer header of a Security Layer packet is equal to '00' (i.e., BATI).
- Otherwise, the access terminal shall discard the Security Layer packet.

8.2.6 Header Formats

8.2.6.1 MAC Layer Header Format

The access network shall place the following header in front of every transmitted Security Layer packet:

Field	Length (bits)
Length	8
SecurityLayerFormat	1
ConnectionLayerFormat	1
Reserved	4
ATI Record	2 or 34

Length The access network shall set this field to the combined length, in octets, of the Security Layer packet and this MAC Layer header excluding the Length field.

SecurityLayerFormat
The access network shall set this field to '1' if security layer packet has security applied; otherwise, the access network shall set this field to '0'.

ConnectionLayerFormat
The access network shall set this field to '1' if the connection layer packet is Format B; otherwise, the access network shall set this field to '0'.

Reserved The access network shall set this field to all zeros. The access terminal shall ignore this field.

ATI Record Access Terminal Identifier Record. The access network shall set this field to the record specifying the access terminal's address. This record is defined in 10.2.

8.2.6.2 Control Channel Header Format

The access network shall place the following header in front of every Control Channel MAC Layer packet:

Field	Length (bits)
SynchronousCapsule	1
LastPacket	1
Offset	2
Reserved	4

SynchronousCapsule
For the first Control Channel MAC Layer packet of a synchronous

capsule, the access network shall set this field to '1'; otherwise, the access network shall set this field to '0'.

LastPacket For the last Control Channel MAC Layer packet of a synchronous capsule or asynchronous capsule, the access network shall set this field to '1'; otherwise, the access network shall set this field to '0'.

Offset For the first Control Channel MAC Layer packet of a synchronous capsule, the access network shall set this field to the offset in slots of the Synchronous Control Channel relative to the Control Channel Cycle; otherwise, the access network shall set this field to zero.

Reserved The access network shall set this field to zero. The access terminal shall ignore this field.

8.2.6.3 Pad

The access network shall add sufficient padding so that the Control Channel MAC Layer packet including all payload and headers is 1000 bits long.

The access network shall set the padding bits to '0'. The access terminal shall ignore the padding bits.

8.2.6.4 Reserved

The access network shall add 2 reserved bits.

The access network shall set the reserved bits to '0'. The access terminal shall ignore the reserved bits.

8.2.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{CCMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{CCMPDefault}$	Subtype field for this protocol	0x0000
$T_{CCMPSupervision}$	Control Channel supervision timer value	12 Control Channel Cycles

8.2.8 Interface to Other Protocols

8.2.8.1 Commands

This protocol does not issue any commands.

8.2.8.2 Indications

This protocol does not register to receive any indications.

8.3 Default Access Channel MAC Protocol

8.3.1 Overview

The Default Access Channel MAC Protocol provides the procedures and messages required for an access terminal to transmit and an access network to receive the Access Channel.

This specification assumes that the access network has one instance of this protocol for all access terminals.

This protocol can be in one of two states:

- Inactive State: In this state the protocol waits for an ***Activate*** command. This state corresponds only to the access terminal and occurs when the access terminal has not acquired an access network or the access terminal has a connection open.
- Active State: In this state the access terminal transmits and the access network receives the Access Channel.

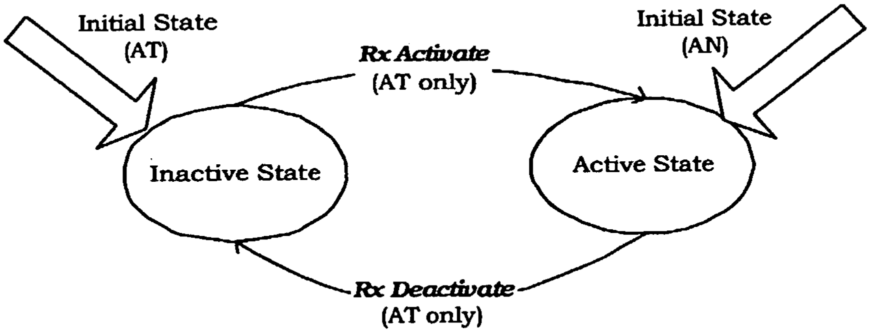


Figure 8.3.1-1. Default Access Channel MAC Protocol State Diagram

8.3.2 Primitives and Public Data

8.3.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***

8.3.2.2 Return Indications

This protocol returns the following indications:

- ***TransmissionSuccessful***
- ***TransmissionAborted***
- ***TransmissionFailed***
- ***TxStarted***

- ***TxEnded***
- ***SupervisionFailed***

8.3.2.3 Public Data

This protocol shall make the following data public:

- DataOffsetNom
- DataOffset9k6
- PowerStep
- OpenLoopAdjust
- ProbeInitialAdjust
- PreambleLength
- AccessSignature field of the next AccessParameters message that it will send
- MI_{ACMAC}
- MQ_{ACMAC}

8.3.3 Basic Protocol Numbers

The Type field for the Access Channel MAC Protocol is one octet, set to $N_{ACMPType}$.

The Subtype field for the Default Access Channel MAC Protocol is two octets, set to $N_{ACMPDefault}$.

8.3.4 Protocol Data Unit

The transmission unit of this protocol is the Access Channel MAC Layer packet. Each Access Channel MAC Layer packet contains part or all of a Security Layer packet.

The protocol constructs one or more packets out of the Security Layer packet as follows:

- it adds the MAC Layer header specified in 8.3.6.1 in front of the Security Layer packet,
- it adds the FCS as defined in 8.3.6.2,
- it pads the Security Layer packet as defined in 8.3.6.3,
- it splits the result into one or more Access Channel MAC Layer capsule fragments,
- it adds the reserved bits, as defined in 8.3.6.4, to the capsule fragments to construct the Access Channel MAC Layer packets.

This protocol passes the packets for transmission to the Physical Layer. An example of the packet structure is shown in Figure 8.3.4-1.

Received packets are passed for further processing to the Security Layer after concatenation, removing the padding, FCS checking, and removing the MAC layer headers. The value of the SecurityLayerFormat and ConnectionLayerFormat fields shall be passed to the Security Layer with the Security Layer packet.

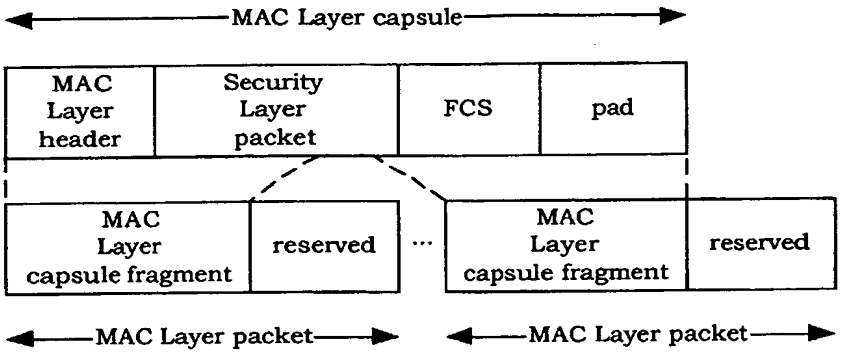


Figure 8.3.4-1. Access Channel MAC Packet Structure

8.3.5 Procedures

8.3.5.1 Protocol Initialization and Configuration

The access terminal shall start this protocol in the Inactive State.

The access network shall start this protocol in the Active State.

Access Channel parameters are provided by using the AccessParameters message, by using the ConfigurationRequest/ConfigurationResponse messages, or by using a protocol constant. Section 8.3.6.6 defines the AccessParameters message. Section 8.3.6.7.1.1 defines the complex attribute that can be configured and the default values the access terminal shall use unless superceded by a configuration exchange (see 10.3). Section 8.3.7 lists the protocol constants.

8.3.5.2 Command Processing

The access network shall ignore all commands.

8.3.5.2.1 Activate

If this protocol receives an ***Activate*** command in the Inactive State,

- The access terminal shall transition to the Active State.
- The access network shall ignore it.

If this protocol receives the command in the Active State it shall be ignored.

8.3.5.2.2 Deactivate

If this protocol receives a ***Deactivate*** command in the Inactive State, it shall be ignored.

If this protocol receives the command in the Active State,

- The access terminal shall transition to the Inactive State.

- The access network shall ignore it.

8.3.5.3 Access Channel Structure

Figure 8.3.5.3-1 and Figure 8.3.5.3-2 illustrate the access probe structure and the access probe sequence.

The Access Channel Cycle specifies the time instants at which the access terminal may start an access probe. An Access Channel probe may only begin at times T such that

$$T \bmod \text{AccessCycleDuration} = 0,$$

where T is system time in slots.

The structure of an individual access probe is shown in Figure 8.3.5.3-1. In each access probe, the pilot (I-channel) is first enabled and functions as a preamble. After PreambleLength frames (PreambleLength × 16 slots), the probe data (Q-channel) is enabled for up to CapsuleLengthMax × 16 slots.

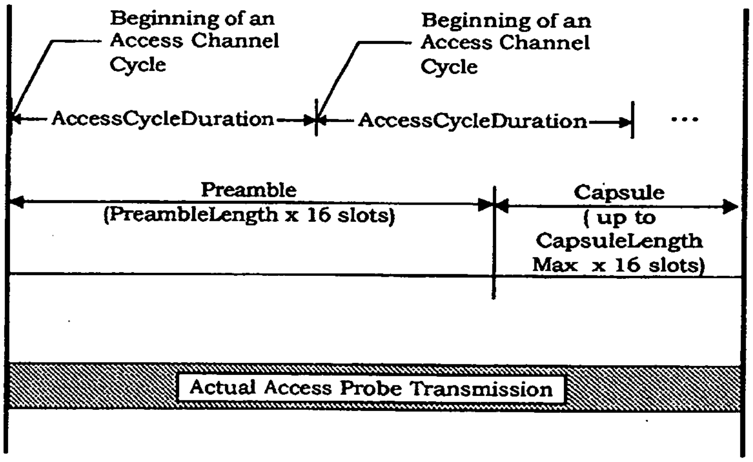

Beginning of an Access Channel Cycle
Beginning of an Access Channel Cycle
AccessCycleDuration
AccessCycleDuration
...
Preamble (PreambleLength x 16 slots)
Capsule (up to CapsuleLength Max x 16 slots)
Actual Access Probe Transmission

Figure 8.3.5.3-1. Access Probe Structure

Each probe in a sequence is transmitted at increased power until any of the following conditions are met:

- Access terminal receives an ACAck message.
- Transmission is aborted because the protocol received a ***Deactivate*** command, or
- Maximum number of probes per sequence (ProbeNumStep) has been transmitted.

Prior to the transmission of the first probe, the access terminal performs a persistence test which is used to control congestion on the Access Channel.

Additionally the access terminal performs a persistence test in between probe sequences.

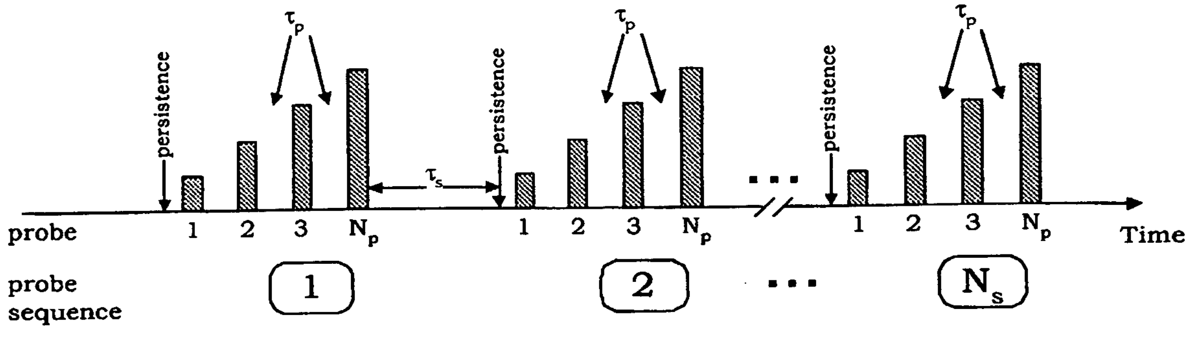


Figure 8.3.5.3-2. Access Probe Sequences

8.3.5.4 Inactive State

This state applies only to the access terminal.

In this state the access terminal waits for an ***Activate*** command.

8.3.5.5 Active State

In this state the access terminal is allowed to transmit on the Access Channel and the access network is monitoring the Access Channel.

If the protocol receives a ***Deactivate*** command,

- Access terminal shall:
  - Immediately cease transmitting on the Access Channel if it is in the process of sending a probe.
  - Return a ***TransmissionAborted*** indication if it was in the process of sending an Access Channel MAC Layer packet.
  - Transition to the Inactive State.
- Access network shall ignore this command.

All other commands shall be ignored in this state.

8.3.5.5.1 Access Terminal Requirements

This protocol enforces a stop and wait packet transmission policy over the Access Channel. That is, the access terminal shall not send a new Access Channel MAC Layer packet before either:

- Receipt of an ACAck message for the previous packet, or
- transmission of the previous packet failed after transmitting ProbeSequenceMax probe sequences for it.

The access terminal shall return a ***TxStarted*** indication before transmitting the first probe for an Access Channel MAC Layer packet.[39]

The access terminal shall return a ***TxEnded*** indication either:

- Simultaneous with a ***TransmissionAborted*** or a ***TransmissionFailed*** indication, or
- $T_{ACMPTransaction}$ seconds after a ***TransmissionSuccessful*** indication.

8.3.5.5.1.1 Probe Transmission

The access terminal shall conform to the following rules when sending a probe:

1. Current SectorParameters. The access terminal shall verify that the value of SectorSignature field of the latest QuickConfig message is the same as SectorSignature field of the latest SectorParameters message prior to sending the first probe of the first probe sequence. Both SectorSignature values (one belonging to the QuickConfig message and one belonging to the SectorParameters message are public data of the Overhead Messages Protocol).

2. Current AccessParameters. Prior to sending the first probe of the probe sequence, the access terminal shall verify that the last AccessParameters message it received is current, according to the last AccessSignature value given as public data by the Overhead Messages Protocol. If the AccessParameters message is not current, the access terminal shall start the AccessParameters supervision timer for $T_{ACMPAPSupervision}$. If the timer expires before it receives the current AccessParameters message, the access terminal shall return a ***SupervisionFailed*** indication and transition to the Inactive State.

3. ATI Record. The access terminal shall set the ATI and ATIType fields of the ATI Record in the MAC Layer header to TransmitATI.ATI and TransmitATI.ATIType, respectively (TransmitATI is provided as public data by the Address Management Protocol).

4. Probe Power Control. The access terminal shall send the i-th probe in the probe sequence at a power level given by $X_0+(i-1)\times$PowerStep, where X_0 represents the access terminal's open-loop mean output power of the Pilot Channel and is given by

   X_0 = - Mean R_X Power (dBm) + OpenLoopAdjust + ProbeInitialAdjust

   and the Mean R_X Power is estimated throughout the transmission of each probe.

5. Probe Structure. When sending a probe, the access terminal shall transmit PreambleLength frames of pilot only, followed by up to CapsuleLengthMax frames of probe data and pilot. The access terminal shall transmit a single Access Channel Capsule per probe. The access terminal shall not change the probe data contents in between probes.

[39] Higher layer protocols use this indication as a notification that there may be an outstanding transaction on the Access Channel; and, therefore, the access terminal should not go to sleep.

6. Long Code Cover. The access terminal shall use the Access Channel long codes to cover the entire probe. The Access Channel long code is specified in 8.3.5.5.1.2.
7. Inter-Probe Backoff. After sending an access probe within an access probe sequence, the access terminal shall wait for τ_P slots after the end of the access probe before sending the next probe in a probe sequence, where $\tau_P = T_{ACMPATProbeTimeout} + (y \times \text{AccessCycleDuration})$ and y is a uniformly distributed integer random number between 0 and ProbeBackoff. The access terminal shall not send the next probe in this probe sequence if it receives an ACAck message or it has already transmitted ProbeNumStep (N_P in Figure 8.3.5.3-2) probes in this probe sequence.

8.3.5.5.1.2 Access Channel Long Code Mask

The access terminal shall set the Access Channel long masks, MI_{ACMAC} and MQ_{ACMAC} as follows.

The 42-bit masks MI_{ACMAC} and MQ_{ACMAC} are specified in Table 8.3.5.5.1.2-1.

Table 8.3.5.5.1.2-1. Access Channel Long Code Masks

BIT	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
MI_{ACMAC}	1	1	AccessCycleNumber								Permuted (ColorCode | SectorID[23:0])																															
MQ_{ACMAC}	0	0	AccessCycleNumber'								Permuted (ColorCode | SectorID[23:0])'																															

In Table 8.3.5.5.1.2-1:

- SectorID is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe.
- ColorCode is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe.
- AccessCycleNumber is defined as follows:

  AccessCycleNumber = SystemTime mod 256

  Where:

  SystemTime is the CDMA System Time in slots corresponding to the slot in which the first access probe preamble for this access probe is sent. System Time is given as public data of Initialization State Protocol, and

  Permuted(ColorCode | SectorID[23:0])' and AccessCycleNumber' are bitwise complement of Permuted(ColorCode| SectorID[23:0]) and AccessCycleNumber, respectively. Permuted(ColorCode | SectorID[23:0]) is a permutation of the bits in ColorCode | SectorID[23:0] and is defined as follows:

  ColorCode | SectorID[23:0] = $(S_{31}, S_{30}, S_{29}, \ldots, S_0)$

  Permuted(ColorCode | SectorID[23:0]) =
  $(S_0, S_{31}, S_{22}, S_{13}, S_4, S_{26}, S_{17}, S_8, S_{30}, S_{21}, S_{12}, S_3, S_{25}, S_{16}, S_7, S_{29}, S_{20}, S_{11}, S_2, S_{24}, S_{15}, S_6, S_{28}, S_{19}, S_{10}, S_1, S_{23}, S_{14}, S_5, S_{27}, S_{18}, S_9)$.

8.3.5.5.1.3 Probe Sequence Transmission

The access terminal shall conform to the following rules when sending a probe sequence:

1. Persistence Test. Prior to sending the first probe of the sequence, the access terminal shall perform a persistence test in each Access Channel Cycle. For this test, the access terminal shall use the value *p* as specified by APersistence[*i*] where *i* is the class of the access terminal and APersistence[*i*] is the $i+1)^{st}$ occurrence of the APersistence field in the AccessParameters message.[40] If the access terminal does not have a class defined, it shall use $i = 0$, corresponding to non-emergency access terminals.

   When *p* is not zero, the persistence test consists of comparing a uniformly distributed random number *x*, $0< x< 1$, with *p*. If $x< p$ the test is said to succeed. If the persistence test succeeds or if the number of consecutive unsuccessful persistence tests exceeds $4/p$, the access terminal may transmit in this Access Channel Cycle. Otherwise, if *p* is not equal to zero, the access terminal shall repeat the persistence test in the next Access Channel Cycle. If *p* is equal to zero, the access terminal shall return a ***TransmissionFailure*** indication and end the access.

2. Transmitter Power. The access terminal shall not transmit a probe if it cannot transmit the probe at the prescribed power. If the access terminal does not transmit a probe for this reason, it shall abort the probe sequence. Aborted probe sequences are counted as part of the total ProbeSequenceMax probe sequences the access terminal is allowed to transmit for a given access.

3. Probe Contents. The access terminal shall not change the data portion of the probe contents between probe sequences.

4. Success Condition. If the access terminal receives an ACAck message it shall stop the probe sequence, including any transmission in progress, and shall return a ***TransmissionSuccessful*** indication.

5. Failure Condition. If the access terminal has already sent ProbeSequenceMax probe sequences for this access (N_S in Figure 8.3.5.3-2), and if it does not receive an ACAck message acknowledging its receipt within $(T_{ACMPATProbeTimeout} + T_{ACMPCycleLen})$ slots after the end of the last access probe, the access terminal shall return a ***TransmissionFailed*** indication and abort the access.

6. Inter-Sequence Backoff. The access terminal shall generate a uniformly distributed integer random number *k* between 0 and ProbeSequenceBackoff. The access terminal shall wait for $\tau_S = (k \times \text{AccessCycleDuration}) + T_{ACMPATProbeTimeout}$ slots from the end of the last probe of the previous sequence before repeating this sequence.

[40] The access terminal's class is configured through means that are outside the scope of this specification.

8.3.5.5.2 Access Network Requirements

The access network should send an AccessParameters message at least once every $N_{ACMPAccessParameters}$ slots.

The access network should send an ACAck message in response to every Access Channel MAC Layer capsule it receives. The message should be sent within $T_{ACMPANProbeTimeout}$ slots of receipt of the packet.

The access network should monitor and control the load on the Access Channel. The access network may control the load by adjusting the access persistence vector, APersistence, sent as part of the AccessParameters message.

8.3.6 Header and Message Formats

8.3.6.1 MAC Layer Header

The access terminal shall place the following header in front of the Security Layer packet:

Field	Length (bits)
Length	8
SessionConfigurationToken	16
SecurityLayerFormat	1
ConnectionLayerFormat	1
Reserved	4
ATI Record	34

Length The access terminal shall set this field to the combined length, in octets, of the Security Layer packet and this MAC Layer header. excluding the Length field.

SessionConfigurationToken
The access terminal shall set this field to the value of the SessionConfigurationToken which is public data of the Session Configuration Protocol.

SecurityLayerFormat
The access terminal shall set this field to '1' if security layer packet has security applied; otherwise, the access terminal shall set this field to '0'.

ConnectionLayerFormat
The access terminal shall set this field to '1' if the connection layer packet is Format B; otherwise, the access terminal shall set this field to '0'.

Reserved	The access terminal shall set this field to zero. The access network shall ignore this field.

ATI Record	Access Terminal Identifier Record. The access terminal shall set this field to the record specifying the access terminal's ID specified by TransmitATI.ATI and TransmitATI.ATIType. This record is defined in 10.2.

8.3.6.2 FCS

The FCS shall be calculated using the standard CRC-CCITT generator polynomial:

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x^{1} + 1$$

The FCS shall be equal to the value computed by the following procedure and the logic shown below:

- All shift register elements shall be initialized to logical zeros.
- Switches shall be set in the up position.
- Register shall be clocked once for each bit of Access Channel MAC Layer Capsule, excluding the FCS and padding bits. The Access Channel MAC Layer Capsule is read in order from MSB to LSB, starting with the MSB of the MAC Layer header
- Switches shall be set in the down position so that the output is a modulo-2 addition with a '0' and the successive shift register inputs are '0'.
- Register shall be clocked an additional 32 times for the 32 FCS bits.

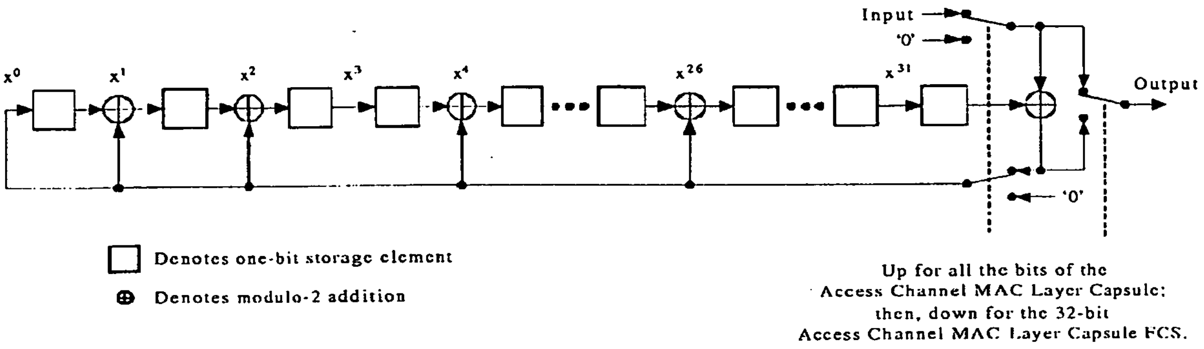

Input
'0'
x^0
x^1
x^2
x^3
x^4
x^{26}
x^{31}
Output
'0'
Denotes one-bit storage element
Denotes modulo-2 addition
Up for all the bits of the Access Channel MAC Layer Capsule; then, down for the 32-bit Access Channel MAC Layer Capsule FCS.

Figure 8.3.6.2-1. Access Channel MAC Layer Capsule FCS

8.3.6.3 Padding Bits

The access terminal shall add sufficient padding so that the Access Channel MAC capsule, including all payload, FCS, padding, and headers, is the smallest possible integer multiple of 232 bits. The access terminal shall set the padding bits to '0'. The access network shall ignore the padding bits.

8.3.6.4 Reserved Bits

The access terminal shall add 2 reserved bits to each Access Channel capsule fragment.

The access terminal shall set the reserved bits to '0'. The access network shall ignore the reserved bits.

8.3.6.5 ACAck

The access network sends the ACAck message to acknowledge receipt of an Access Channel MAC Layer capsule.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x00.

Channels	CC	SLP	Best Effort
Addressing	unicast	Priority	10

8.3.6.6 AccessParameters

The AccessParameters message is used to convey Access Channel information to the access terminals.

Field	Length (bits)
MessageID	8
AccessCycleDuration	8
AccessSignature	16
OpenLoopAdjust	8
ProbeInitialAdjust	5
ProbeNumStep	4
PreambleLength	3

$N_{ACMPAPersist}$ occurrences of the following field:

APersistence	6

Reserved	variable

MessageID The access network shall set this field to 0x01.

AccessCycleDuration
The access network shall set this field to the duration of an Access Channel Cycle in units of slots.

AccessSignature
AccessParameters message signature. The access network shall change this field if the contents of the AccessParameters message change.

OpenLoopAdjust
The access network shall set this field to the negative of the nominal power to be used by access terminals in the open loop power estimate, expressed as an unsigned value in units of 1 dB.

ProbeInitialAdjust
The access network shall set this field to the correction factor to be used by access terminals in the open loop power estimate for the initial transmission on the Access Channel, expressed as a two's complement value in units of 1 dB.

ProbeNumStep
The access network shall set this field to the maximum number of access probes access terminals are to transmit in a single access probe sequence. The access network shall set this field to a value in the range [1 ... 15].

PreambleLength
The access network shall set this field to the length in frames of the access probe preamble.

APersistence
Access persistence vector. If a value in this vector is 0x3F, the access terminal shall use zero as the corresponding persistence probability; otherwise, if the value of this field, *n*, not equal to 0x3F, the access terminal shall use $2^{-n/4}$ as the corresponding persistence probability.

Reserved
Number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC
Addressing	Broadcast

SLP	Best Effort
Priority	30

8.3.6.7 Configuration Messages

The Default Access Channel MAC Protocol uses the Generic Configuration Protocol to transmit configuration parameters from the access network to the access terminal.

8.3.6.7.1 Configurable Attributes

8.3.6.7.1.1 The following complex attributes and default values are defined (see 10.3):InitialConfiguration

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
CapsuleLengthMax	4	2
PowerStep	4	6
ProbeSequenceMax	4	3
ProbeBackoff	4	4
ProbeSequenceBackoff	4	8
Reserved	4	N/A

Length — Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — Parameter set identifier. The access network shall set this field to 0x00.

ValueID — The access network shall set this field to an identifier assigned to this complex attribute. The access network should change this field for each set of values for this complex attribute.

CapsuleLengthMax — Access Channel Capsule length. The access network shall set this field to the maximum number of frames in an Access Channel Capsule. The access terminal shall support all the valid values specified by this field.

PowerStep — Probe power increase step. The access network shall set this field to the increase in power between probes, in resolution of 0.5 dB. The access terminal shall support all the valid values specified by this field.

ProbeSequenceMax — Maximum number of probe sequences. The access network shall set this field to the maximum number of probe sequences for a single access attempt. The access terminal shall support all the valid values specified by this field.

ProbeBackoff Inter-probe backoff. The access network shall set this field to the upper limit of the backoff range (in units of AccessCycleDuration) that the access terminal is to use between probes. The access terminal shall support all the valid values specified by this field.

ProbeSequenceBackoff

Inter-probe sequence backoff. The access network shall set this field to the upper limit of the backoff range (in units of AccessCycleDuration) that the access terminal is to use between probe sequences. The access terminal shall support all the valid values specified by this field.

Reserved The access network shall set this field to zero. The access terminal shall ignore this field.

8.3.6.7.1.2 PowerParameters Attribute

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
DataOffsetNom	4	0
DataOffset9k6	4	0

Length Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID The access network shall set this field to 0x01.

ValueID The access network shall set this field to an identifier assigned to this complex value.

DataOffsetNom The access network shall set this field to the nominal offset of the access data channel power to pilot channel power, expressed as 2's complement value in units of 0.5 dB. The access terminal shall support all the valid values specified by this field.

DataOffset9k6 The access network shall set this field to the ratio of access channel power at 9600 bps to the nominal access channel power at 9600 bps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field.

8.3.6.7.2 ConfigurationRequest

The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x50.

Channels	CC FTC
Addressing	unicast

SLP	Reliable
Priority	40

8.3.6.7.3 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the access terminal includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response and it shall set the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

Channels	RTC	SLP	Reliable
Addressing	unicast	Priority	40

8.3.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{ACMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{ACMPDefault}$	Subtype field for this protocol	0x0000
$N_{ACMPAPersist}$	Number of different persistence values	4
$N_{ACMPAccessParameters}$	The recommended maximum number of slots between transmission of two consecutive AccessParameters message.	3 * $T_{ACMPCycleLen}$
$T_{ACMPAPSupervision}$	AccessParameters supervision timer	12 * $T_{ACMPCycleLen}$
$T_{ACMPATProbeTimeout}$	Time to receive an acknowledgment at the access terminal for a probe before sending another probe	128 slots
$T_{ACMPANProbeTimeout}$	Maximum time to send an acknowledgment for a probe at the access network	96 slots
$T_{ACMPTransaction}$	Time for access terminal to wait after a successful transmission before returning a ***TxEnded*** indication	1 second
$T_{ACMPCycleLen}$	Length of Control Channel Cycle	256 slots

8.3.8 Interface to Other Protocols

8.3.8.1 Commands

This protocol does not issue any commands.

8.3.8.2 Indications

This protocol does not register to receive any indications.

8.4 Default Forward Traffic Channel MAC Protocol

8.4.1 Overview

The Default Forward Traffic Channel MAC Protocol provides the procedures and messages required for an access network to transmit and an access terminal to receive the Forward Traffic Channel. Specifically, this protocol addresses Forward Traffic Channel addressing and Forward Traffic Channel rate control.

The access network maintains an instance of this protocol for every access terminal.

This protocol operates in one of three states:

- Inactive State: In this state, the access terminal is not assigned a Forward Traffic Channel. When the protocol is in this state, it waits for an ***Activate*** command.
- Variable Rate State: In this state, the access network transmits the Forward Traffic Channel at a variable rate, as a function of the access terminal's DRC value.
- Fixed Rate State: In this state, the access network transmits the Forward Traffic Channel to the access terminal from one particular sector, at one particular rate.

The protocol states and allowed transitions between the states are shown in Figure 8.4.1-1. The rules governing these transitions are provided in sections 8.4.5.1, 8.4.5.4, 8.4.5.5.2, and 8.4.5.6.3 for transitions out of the Inactive State, Variable Rate State, and Fixed Rate State.

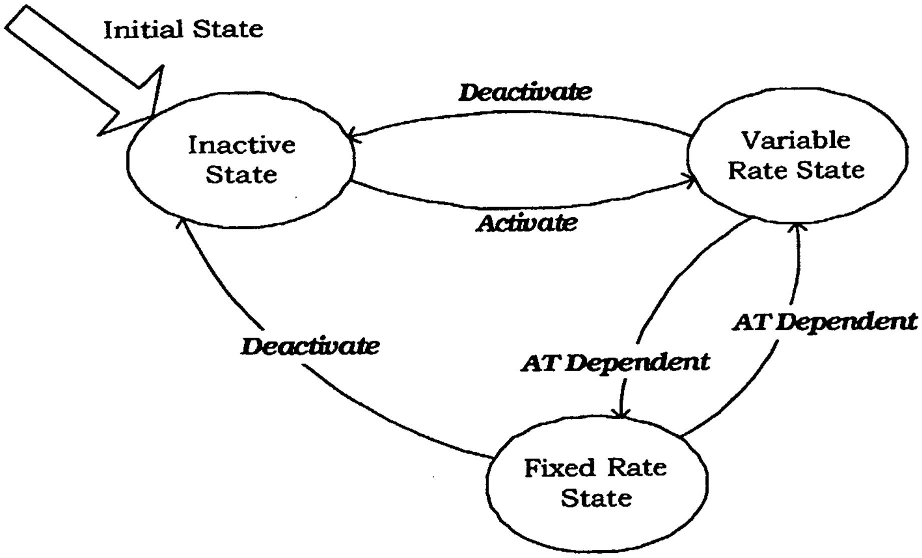


Figure 8.4.1-1. Forward Traffic Channel MAC Protocol State Diagram

8.4.2 Primitives and Public Data

8.4.2.1 Commands

This protocol defines the following commands:

- ***Activate***
- ***Deactivate***

8.4.2.2 Return Indications

This protocol returns the following indications:

- ***SupervisionFailed***

8.4.2.3 Public Data

This protocol shall make the following data public:

- DRCGating
- DRCLength
- DRCChannelGain
- AckChannelGain
- DRCCover for every pilot in the Active Set
- Transmission rate in the Fixed Rate State

8.4.3 Basic Protocol Numbers

- Type field for this protocol is one octet, set to $N_{FTCMPType}$
- Subtype field for this protocol is two octets, set to $N_{FTCMPDefault}$

8.4.4 Protocol Data Unit

The transmission unit of this protocol is a Forward Traffic Channel MAC Layer packet. Each packet consists of one Security Layer packet.

The protocol constructs a Forward Traffic Channel MAC Layer packet out of the Security Layer packet by adding the MAC Layer trailer as defined in 8.4.6.1.

The protocol then sends the packet for transmission to the Physical Layer. The packet structure is shown in Figure 8.4.4-1.

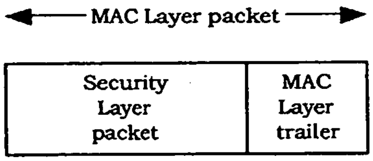


Figure 8.4.4-1. Forward Traffic Channel MAC Layer Packet Structure

If the MACLayerFormat field of the MAC Layer trailer is equal to '1', received packets are passed for further processing to the Security Layer after removing the layer-related trailer. The access terminal shall discard the MAC packet if the MACLayerFormat field of the MAC Layer trailer is equal to '0'. The ConnectionLayerFormat field within the MAC Layer trailer shall be passed to the Security Layer with the Security Layer packet.

8.4.5 Procedures

8.4.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

The parameters for the Default Forward Traffic Channel MAC protocol are provided by using the ConfigurationRequest/ConfigurationResponse messages or by using a protocol constant. Section 8.4.6.4 defines the attributes that can be configured and the default values that the access terminal shall use unless superseded by a configuration exchange. Section 8.4.7 lists the protocol constants.

8.4.5.2 Command Processing

8.4.5.2.1 Activate

If this protocol receives an ***Activate*** command in the Inactive State, the access terminal and the access network shall transition to the Variable Rate State.

If this protocol receives the command in any other state it shall be ignored.

8.4.5.2.2 Deactivate

If the protocol receives a ***Deactivate*** command in the Variable Rate State or the Fixed Rate State,

- The access terminal shall cease monitoring the Forward Traffic Channel, shall cease transmitting the DRC Channel, and shall transition to the Inactive State.
- The access network should cease transmitting the Forward Traffic Channel to this access terminal, should cease receiving the DRC channel from this access terminal, and should transition to the Inactive State.

If this command is received in the Inactive State it shall be ignored.

8.4.5.3 Forward Traffic Channel Addressing

Transmission on the Forward Traffic Channel is time division multiplexed. At any given time, the channel is either being transmitted or not; and, if it is being transmitted, it is addressed to a single user. When transmitting the Forward Traffic Channel, the access network uses the MACIndex to identify the target access terminal.

Requirements for Forward Traffic Channel addressing are part of the Physical Layer.

8.4.5.4 Inactive State

When the protocol is in the Inactive State, the access terminal and the access network wait for an ***Activate*** command.

8.4.5.5 Variable Rate State

In the Variable Rate State, the access network transmits at the rate dictated by the Data Rate Control (DRC) Channel transmitted by the access terminal. The access terminal shall use either a DRC cover index 0 or the DRC Cover index associated with a sector in its Active Set. The DRC cover index 0 is called the "null cover". A DRC cover that corresponds to a sector in the access terminal's Active Set is called a "sector cover". The access terminal is said to be pointing the DRC at a sector in its Active Set if the access terminal is using the DRC cover corresponding to that sector.

The access terminal shall perform the supervision procedures described in 8.4.5.7 in the Variable Rate State.

8.4.5.5.1 DRC and Packet Transmission Requirements

The access terminal uses the DRC cover to specify the transmitting sector (the access terminal is said to point the DRC at that sector). The access terminal uses the DRC value to specify the requested transmission rate.

8.4.5.5.1.1 Access Terminal Requirements

The access terminal shall obey the following rules when transmitting the DRC:

- access terminal shall use DRCLength slots to send a single DRC.
- The DRC value and/or cover may change in slots T such that:

  (T + 1 – FrameOffset) mod DRCLength = 0

  where T is the system time in slots.
- If the DRCGating is equal to 1, the access terminal shall transmit the DRC over a one slot period, starting in slot T that satisfies the following equation:

  (T + 2 – FrameOffset) mod DRCLength = 0
- DRC cover shall obey the following rules:
  - If the access terminal's current DRC cover is a sector cover, then the access terminal's next DRC cover shall not be a different sector cover. It may only be the same sector cover or a null cover.
  - If the access terminal's most recent sector cover corresponds to sector A, then the access terminal shall not use a sector cover corresponding to a sector B until the access terminal has determined that packets received from sector B will not overlap in time with packets received from sector A.

- The access terminal may inhibit reception of data from the access network by covering the DRC with the null cover. The access terminal shall set the DRC to the value it would have used had it requested data from the best serving sector.
- The access terminal shall use either the null cover or a sector cover (see 8.4.5.5) as DRC cover.

- Access terminal shall set the DRC to one of the valid values in Table 8.4.5.5.1.1-1, corresponding to the rate it requests.
- Access terminal shall set the DRC to the maximum value that channel conditions permit for the sector at which the access terminal is pointing its DRC. The access terminal uses the null rate if the channel conditions do not permit even the lowest non-null rate.

Table 8.4.5.5.1.1-1. DRC Value Specification

DRC value	Rate (kbps)	Packet Length (Slots)
0x0	null rate	N/A
0x1	38.4	16
0x2	76.8	8
0x3	153.6	4
0x4	307.2	2
0x5	307.2	4
0x6	614.4	1
0x7	614.4	2
0x8	921.6	2
0x9	1228.8	1
0xa	1228.8	2
0xb	1843.2	1
0xc	2457.6	1
0xd	Invalid	N/A
0xe	Invalid	N/A
0xf	Invalid	N/A

- If the access terminal has finished sending its DRC to sector A during slot n specifying a requested rate r, the access terminal should search for a preamble transmitted at rate $r$from sector A during slots n + 1 through n + DRCLength.

- If the access terminal detects a preamble from any sector, the access terminal shall continue to receive the entire packet from that sector, using the requested rate.
- If the access terminal is not already receiving a packet, it shall attempt to receive a packet transmitted at the rate it requested through the corresponding DRC value.
- If the access terminal receives a DRCLock bit that is set to '0' from the sector to which it is pointing its DRC, the access terminal should stop pointing its DRC at that sector.

8.4.5.5.1.2 Access Network Requirements

The access network shall obey the following rules when processing the DRC and sending a packet to the access terminal:

- If the access network begins transmitting a packet to the access terminal at slot T, it shall do so at the rate specified by the DRC whose reception was completed in slot T - 1 - ((T - FrameOffset) mod DRCLength).
- Once the access network initiates a packet transmission to a particular access terminal, it shall continue transmitting to that access terminal until it receives a *PhysicalLayer.ForwardTrafficCompleted* indication.

8.4.5.5.2 Transitions from the Variable Rate State

The access terminal may transition to the Fixed Rate State at any time. The access terminal shall perform the following steps in order to transition to the Fixed Rate State.

- If the access terminal's last sector cover was sector A, then the access terminal shall continue using sector A's cover until it has determined that it is no longer going to be served by Sector A.
- Then, the access terminal shall cover the DRC with the null cover.
- Then, the access terminal shall send the FixedModeRequest message specifying:
  - A sector in the active set.
  - A data rate.

8.4.5.6 Fixed Rate State

In the Fixed Rate State, the access terminal receives Forward Traffic Channel MAC Layer packets at a specific rate from a specific sector. When the access network transmits a Forward Traffic Channel MAC Layer packet to the access terminal, it uses the specified sector at the specified rate.

The access network shall perform at least one of the following actions within $T_{FTCMPANFixedMode}$ seconds of entering the Fixed Rate State:

- Transmit a packet to the access terminal on the Forward Traffic Channel, or
- Send a FixedModeResponse message to the access terminal, specifying the TransactionID of the last FixedModeRequest message it received.

Upon entering the Fixed Rate State, the access terminal shall set a transition timer for $T_{FTCMPATFixedMode}$ seconds.

If the transition timer is enabled and the access terminal receives a FixedModeResponse message or a valid packet on the Forward Traffic Channel, the access terminal shall disable this timer.

If the transition timer expires, the access terminal shall transition to the Variable Rate State by covering its DRC with a sector cover (see 8.4.5.6.3). The term "sector cover" is defined in 8.4.5.5.

The access terminal shall perform the supervision procedures described in 8.4.5.7 in the Fixed Rate State.

8.4.5.6.1 DRC Requirements

The access terminal shall cover the DRC with the null cover. The null cover is defined in 8.4.5.5.

The access terminal shall set the DRC value to the value it would have requested from this serving sector, had it been in the Variable Rate State.

8.4.5.6.2 Packet Transmission

The access network shall only schedule Forward Traffic Channel MAC Layer packet transmissions to the access terminal on the Forward Traffic Channel transmitted by the sector specified in the FixedModeRequest message. The access network shall send the packet at the rate specified in the FixedModeRequest message. If the access network begins a packet transmission, it shall continue transmitting the packet until it receives a ***PhysicalLayer.ForwardTrafficCompleted*** indication. The access terminal shall monitor the Forward Traffic Channel transmitted by the sector specified in the FixedModeRequest message.

8.4.5.6.3 Transitions from the Fixed Rate State

In order to transition to the Variable Rate State, the access terminal shall cover its DRC with a sector cover.The access terminal shall transition to the Variable Rate State if the sector specified in the FixedModeRequest message is no longer a member of the access terminal's Active Set.

8.4.5.7 Supervision Procedures

8.4.5.7.1 DRC Supervision

The access terminal shall perform supervision on the DRC as follows:

- The access terminal shall set the DRC supervision timer for $T_{FTCMDRCSupervision}$ when it transmits a null rate DRC.
- If the access terminal requests a non-null rate while the DRC supervision timer is active, the access terminal shall disable the timer.

- If the DRC supervision timer expires, the access terminal shall disable the Reverse Traffic Channel transmitter and set the Reverse Traffic Channel Restart timer for time $T_{FTCMPRestartTx}$.
- If the access terminal generates consecutive non-null rate DRC values for more than $_{FTCMPRestartTx}$ slots, the access terminal shall disable the Reverse Traffic Channel Restart timer and shall enable the Reverse Traffic Channel transmitter.
- If the Reverse Traffic Channel Restart timer expires, the access terminal shall return a ***SupervisionFailed*** indication and transition to the Inactive State.

8.4.5.7.2 ForwardTrafficValid Monitoring

The access terminal shall monitor the bit associated with its MACIndex in the ForwardTrafficValid field made available by the Overhead Messages protocol. If this bit is set to 0, the access terminal shall return a ***SupervisionFailed*** indication and transition to the Inactive State.

8.4.6 Trailer and Message Formats

8.4.6.1 MAC Layer Trailer

The access network shall set the MAC Layer Trailer as follows:

Field	Length (bits)
ConnectionLayerFormat	1
MACLayerFormat	1

ConnectionLayerFormat
The access network shall set this field to '1' if the connection layer packet is Format B; otherwise, the access network shall set this field to '0'.

MACLayerFormat The access network shall set this field to '1' if the MAC layer packet contains a valid payload; otherwise, the access network shall set this field to '0'.

8.4.6.2 FixedModeRequest

The access terminal sends the FixedModeRequest message to indicate a transition to the Fixed Rate State.

Field	Length (bits)
MessageID	8
TransactionID	8
DRCCover	3
RequestedRate	4
Reserved	1

MessageID The access terminal shall set this field to 0x00.

TransactionID The access terminal shall increment this field every time it sends a new FixedModeRequest message.

DRCCover The access terminal shall set this field to the DRC cover associated with the sector in its Active Set from which it wants to receive packets on the Forward Traffic Channel.

RequestedRate The access terminal shall set this field to one of the valid DRC values in Table 8.4.5.5.1.1-1 to indicate the rate at which it wants to receive packets.

Reserved The access terminal shall set this field to zero. The access network shall ignore this field.

Channels	RTC	SLP	Reliable
Addressing	unicast	Priority	40

8.4.6.3 FixedModeResponse

The access network sends the FixedModeResponse message to acknowledge the transition to the Fixed Rate State.

Field	Length (bits)
MessageID	8
TransactionID	8

MessageID The access network shall set this field to 0x01.

TransactionID The access network shall set this field to the TransactionID field of the associated FixedModeRequest message.

Channels	CC	FTC
Addressing		unicast

SLP	Reliable
Priority	40

8.4.6.4 Configuration Messages

The Default Forward Traffic Channel MAC Protocol uses the Generic Configuration Protocol to exchange configuration parameters between the access network and the access terminal (see 10.7).

8.4.6.4.1 Configurable Attributes

The following attributes and default values are defined:

8.4.6.4.1.1 Simple Attributes

The negotiable simple attribute for this protocol is listed in Table 8.4.6.4-1. The access terminal shall use as defaults the values in Table 8.4.6.4-1 typed in ***bold italics***.

Table 8.4.6.4-1. Configurable Values

Attribute ID	Attribute	Values	Meaning
0xff	DRCGating	*0x0000*	Continuous transmission
		0x0001	Discontinuous transmission

The access terminal shall support the default value of this attribute.

8.4.6.4.1.2 HandoffDelays Attribute

The following HandoffDelays complex attribute and default values are defined:

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
SofterHandoffDelay	8	0x08
SoftHandoffDelay	8	0x10

Length

Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID

The access network shall set this field to 0x00.

ValueID

The access network shall set this field to an identifier assigned to this complex value.

SofterHandoffDelay

The access network shall set this field to the minimum interruption seen by the access terminal when the access terminal switches the DRC from a source sector to a target sector where the target sector is such that its Forward Traffic Channel carries the same closed-loop power control bits as the source sector (see SofterHandoff field of the Route Update Protocol TrafficChannelAssignment message). The access network shall specify this field in units of 8 slots. The access terminal may use this number to adjust its algorithm controlling DRC switching. The access terminal shall support all the values of this attribute.

SoftHandoffDelay

The access network shall set this field to the minimum interruption seen by the access terminal when the access terminal switches the DRC from a source sector to a target sector where the target sector is such that its Forward Traffic Channel does not always carry the same closed-loop power control bits as the source sector (see SofterHandoff field of the Route Update Protocol TrafficChannelAssignment message). The access network shall specify this field in units of 8 slots. The access terminal may use this number to adjust its algorithm controlling DRC switching. The access terminal shall support all the values of this attribute.

8.4.6.4.2 ConfigurationRequest

The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x50.

Channels	CC	FTC	RTC
Addressing			unicast

SLP	Reliable
Priority	40

8.4.6.4.3 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the access terminal includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response and shall set the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

Channels	CC	FTC	RTC
Addressing			unicast

SLP	Reliable
Priority	40

8.4.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{FTCMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{FTCMPDefault}$	Subtype field for this protocol	0x0000
$N_{FTCMPRestartTx}$	Number of consecutive slots of non-null rate DRCs to re-enable the Reverse Traffic Channel transmitter once it is disabled due to DRC supervision failure.	16
$T_{FTCMPATFixedMode}$	Time the access terminal waits for the access network to acknowledge a transition to the Fixed Mode State.	1 second
$T_{FTCMPANFixedMode}$	Time the access network has to acknowledge a transition to the Fixed Mode State	0.9 second
$T_{FTCMDRCSupervision}$	DRC supervision timer	240 ms
$T_{FTCMPRestartTx}$	Reverse Channel Restart Timer	12 Control Channel cycles

8.4.8 Interface to Other Protocols

8.4.8.1 Commands Sent

This protocol does not issue any commands.

8.4.8.2 Indications

This protocol registers to receive the following indication:

- ***PhysicalLayer.ForwardTrafficCompleted***

8.5 Default Reverse Traffic Channel MAC Protocol

8.5.1 Overview

The Default Reverse Traffic Channel MAC Protocol provides the procedures and messages required for an access terminal to transmit, and for an access network to receive the Reverse Traffic Channel. Specifically, this protocol addresses Reverse Traffic Channel transmission rules and rate control.

This specification assumes that the access network has one instance of this protocol for every access terminal.

This protocol operates in one of three states:

- Inactive State: In this state, the access terminal is not assigned a Reverse Traffic Channel. When the protocol is in this state, it waits for an ***Activate*** command.
- Setup State: In this state, the access terminal obeys the power control commands that it receives from the access network. Data transmission on the Reverse Traffic Channel is not allowed in this state.
- Open State: In this state, the access terminal may transmit data and negotiate different transmission rates on the Reverse Traffic Channel.

The protocol states and the indications and events causing the transition between the states are shown in Figure 8.5.1-1.

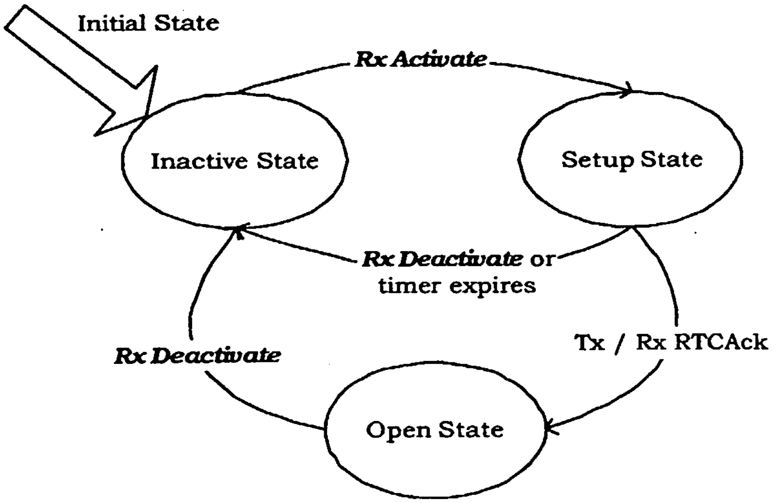


Figure 8.5.1-1. Reverse Traffic Channel MAC Protocol State Diagram

8.5.2 Primitives and Public Data

8.5.2.1 Commands

This protocol defines the following commands:

- *Activate*
- *Deactivate*

8.5.2.2 Return Indications

This protocol returns the following indications:

- *LinkAcquired*

8.5.2.3 Public Data

This protocol shall make the following data public:

- RABLength for every pilot in the Active Set
- RABOffset for every pilot in the Active Set
- DataOffsetNom
- DataOffset9k6
- DataOffset19k2
- DataOffset38k4
- DataOffset76k8
- DataOffset153k6
- RPCStep
- MI_{RTCMAC}
- MQ_{RTCMAC}

8.5.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to $N_{RTCMPType}$.

The Subtype field for this protocol is two octets, set to $N_{RTCMPDefault}$.

8.5.4 Protocol Data Unit

The transmission unit of this protocol is a Reverse Traffic Channel MAC Layer packet. Each packet contains one Security Layer packet.

The protocol constructs a packet out of the Security Layer packets by adding the MAC Layer trailer defined in 8.5.6.1. The protocol then sends the packet for transmission to the Physical Layer. The packet structure is shown in Figure 8.5.4-1

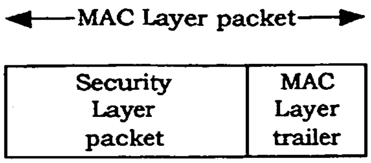


Figure 8.5.4-1. Reverse Traffic Channel MAC Layer Packet Structure

If the MACLayerFormat field of the MAC Layer trailer is equal to '1', received packets are passed for further processing to the Security Layer after removing the layer-related trailer. The access network shall discard the MAC packet if the MACLayerFormat field of the MAC Layer trailer is equal to '0'. The ConnectionLayerFormat field in the MAC Layer trailer shall be passed to the Security Layer with the Security Layer packet.

The maximum size payload this protocol can support (i.e., the maximum size Security Layer packet that can be carried) is a function of the transmission rate used on the Reverse Traffic Channel. Table 8.5.4-1 provides the transmission rates and corresponding minimum and maximum payload sizes available on the Reverse Traffic Channel.

Table 8.5.4-1. Reverse Traffic Channel Rates and Payload

Transmission Rate (kbps)	Minimum Payload (bits)	Maximum Payload (bits)
0.0	0	0
9.6	1	232
19.2	233	488
38.4	489	1000
76.8	1001	2024
153.6	2025	4072

8.5.5 Procedures

8.5.5.1 Protocol Initialization and Configuration

This protocol shall be started in the Inactive State.

Configuration parameters are provided by using the ConfigurationRequest/ConfigurationResponse messages or by using a protocol constant. Section 8.5.6.5.1 defines the attributes that can be configured and the default values that the access terminal shall use unless superseded by a configuration exchange. Section 8.5.7 lists the protocol constants.

8.5.5.2 Command Processing

8.5.5.2.1 Activate

If the protocol receives an ***Activate*** command in the Inactive State, the access terminal and the access network shall perform the following:

- Set ATI_{LCM} to TransmitATI.ATI
- Transition to the Setup State

If the protocol receives this command in any other state it shall be ignored.

8.5.5.2.2 Deactivate

If the protocol receives a ***Deactivate*** command in the Setup State or the Open State,

- Access terminal shall cease transmitting the Reverse Traffic Channel and shall transition to the Inactive State.
- Access network shall cease monitoring the Reverse Traffic Channel from this access terminal and shall transition to the Inactive State.

If the protocol receives a ***Deactivate*** command in the Inactive State, it shall be ignored.

8.5.5.3 Reverse Traffic Channel Long Code Mask

The access terminal shall set the long code masks for the reverse traffic channel (MI_{RTCMAC} and MQ_{RTCMAC}) as shown in Table 8.5.5.3-1.

Table 8.5.5.3-1. Reverse Traffic Channel Long Code Masks

BIT	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01	00
MI_{RTCMAC}	1	1	1	1	1	1	1	1	1	1	Permuted (ATI_{LCM})																															
MQ_{RTCMAC}	0	0	0	0	0	0	0	0	0	0	Permuted (ATI_{LCM})'																															

Permuted (ATI_{LCM}) is defined is follows:

$$ATI_{LCM} = (A_{31}, A_{30}, A_{29}, \ldots, A_0)$$

$$\text{Permuted } (ATI_{LCM}) = (A_0, A_{31}, A_{22}, A_{13}, A_4, A_{26}, A_{17}, A_8, A_{30}, A_{21}, A_{12}, A_3, A_{25}, A_{16}, A_7, A_{29}, A_{20}, A_{11}, A_2, A_{24}, A_{15}, A_6, A_{28}, A_{19}, A_{10}, A_1, A_{23}, A_{14}, A_5, A_{27}, A_{18}, A_9).$$

Permuted (ATI_{LCM})' is bitwise complement of Permuted (ATI_{LCM}).

8.5.5.4 Inactive State

When the protocol is in the Inactive State the access terminal and the access network wait for an ***Activate*** command.

8.5.5.5 Setup State

8.5.5.5.1 Access Terminal Requirements

The access terminal shall set a timer for $T_{RTCMPATSetup}$ seconds when it enters this state. If the protocol is still in the Setup State when the timer expires, the access terminal shall cease transmission on the Reverse Traffic Channel and transition to the Inactive State.

The access terminal shall start transmission on the reverse Traffic Channel upon entering this state, and shall obey the Reverse Power Control Channel. The access terminal shall set the DRC value and cover as specified in the Forward Traffic Channel MAC Protocol.

The access terminal shall not transmit any data on the Reverse Traffic Data Channel while in this state.

If the access terminal receives an RTCAck message it shall return a ***LinkAcquired*** indication and transition to the Open State.

8.5.5.5.2 Access Network Requirements

The access network shall set a timer for $T_{RTCMPANSetup}$ seconds when it enters this state. If the protocol is still in the Setup State when the timer expires, the access network shall transition to the Inactive State.

The access network shall attempt to acquire the Reverse Traffic Channel in this state. If the access network acquires the Reverse Traffic Channel, it shall send an RTCAck message to the access terminal, return a ***LinkAcquired*** indication, and shall transition to the Open State.

8.5.5.6 Open State

8.5.5.6.1 Frame Offset Delay

The access terminal shall delay the Reverse Traffic Data Channel and Reverse Rate Indicator Channel (RRI) transmissions by FrameOffset slots with respect to the system-time-aligned frame boundary.

8.5.5.6.2 Rate Control

The description in this section uses the following variables: MaxRate, CurrentRate, CombinedBusyBit, and CurrentRateLimit.

CurrentRateLimit shall be set initially to 9.6kbps. After a BroadcastReverseRateLimit message or a UnicastReverseRateLimit message is received by the access terminal, the access terminal shall update the CurrentRateLimit value as follows:

- If the RateLimit value in the message is less than or equal to the CurrentRateLimit value, the access terminal shall set CurrentRateLimit to the RateLimit value in the message immediately after the receipt of the message.

- If the RateLimit value in the message is greater than the CurrentRateLimit value, then the access terminal shall set CurrentRateLimit to the RateLimit value in the message, one frame (16 slots) after the message is received.

If the last received reverse activity bit is set to '1' from any sector in the access terminal's active set, the access terminal shall set CombinedBusyBit to '1'. Otherwise, the access terminal shall set CombinedBusyBit to '0'.

CurrentRate shall be set to the rate at which the access terminal was transmitting data immediately before the new transmission time. If the access terminal was not transmitting data immediately before the new transmission time, the access terminal shall set CurrentRate to 0.

The access terminal sets the variable MaxRate based on its current transmission rate, the value of the CombinedBusyBit, and a random number. The access terminal shall generate a random number *x*, uniformly distributed between 0 and 1. The access terminal shall evaluate the condition shown in Table 8.5.5.6.2-1 based on the values of CurrentRate, CombinedBusyBit, and Condition. If the Condition is true, the access terminal shall set MaxRate to the MaxRateTrue value for the corresponding row in Table 8.5.5.6.2-1. Otherwise, the access terminal shall set MaxRate to the MaxRateFalse value for the corresponding row in Table 8.5.5.6.2-1.

Table 8.5.5.6.2-1. Determination of MaxRate

CurrentRate	Combined BusyBit	Condition	MaxRateTrue	MaxRateFalse
0	'0'	True	9.6kbps	N/A
9.6kbps	'0'	$x <$ Transition009k6_019k2	19.2kbps	9.6kbps
19.2kbps	'0'	$x <$ Transition019k2_038k4	38.4kbps	19.2kbps
38.4kbps	'0'	$x <$ Transition038k4_076k8	76.8kbps	38.4kbps
76.8kbps	'0'	$x <$ Transition076k8_153k6	153.6kbps	76.8kbps
153.6kbps	'0'	False	N/A	153.6kbps
0	'1'	False	N/A	9.6kbps
9.6kbps	'1'	False	N/A	9.6kbps
19.2kbps	'1'	$x <$ Transition019k2_009k6	9.6kbps	19.2kbps
38.4kbps	'1'	$x <$ Transition038k4_019k2	19.2kbps	38.4kbps
76.8kbps	'1'	$x <$ Transition076k8_038k4	38.4kbps	76.8kbps
153.6kbps	'1'	$x <$ Transition153k2_076k8	76.8kbps	153.6kbps

The access terminal shall select a transmission rate that satisfies the following constraints:

- The access terminal shall transmit at a rate that is no greater than the value of MaxRate.
- The access terminal shall transmit at a rate that is no greater than the value of CurrentRateLimit.
- The access terminal shall transmit at a data rate no higher than the highest data rate that can be accommodated by the available transmit power.
- The access terminal shall not select a data rate for which the minimum payload length, as specified in Table 8.5.4-1, is greater than the size of data it has to send.

8.5.5.6.3 Power Control

The access terminal shall control the reverse link transmit power in accordance with the requirements of the Physical Layer Protocol.

8.5.6 Trailer and Message Formats

8.5.6.1 MAC Layer Trailer

The access terminal shall set the MAC Layer trailer as follows:

Field	Length (bits)
ConnectionLayerFormat	1
MACLayerFormat	1

ConnectionLayerFormat
The access terminal shall set this field to '1' if the connection layer packet is Format B; otherwise, the access teminal shall set this field to '0'.

MACLayerFormat The access terminal shall set this field to '1' if the MAC layer packet contains a valid payload; otherwise, the access terminal shall set this field to '0'.

8.5.6.2 RTCAck

The access network sends the RTCAck message to notify the access terminal that it has acquired the Reverse Traffic Channel. The access network shall send this message using the access terminal's current ATI.

Field	Length (bits)
MessageID	8

MessageID The access network shall set this field to 0x00.

Channels	CC FTC
Addressing	unicast

SLP	Best Effort
Priority	10

8.5.6.3 BroadcastReverseRateLimit

The BroadcastReverseRateLimit message is used by the access network to control the transmission rate on the reverse link.

Field	Length (bits)
MessageID	8
RPCCount	6

RPCCount occurrences of the following field

RateLimit	4

Reserved	Variable

MessageID The access network shall set this field to 0x01.

RPCCount The access network shall set this value to the maximum number of RPC channels supported by the sector.

RateLimit The access network shall set occurrence ***n*** of this field to the highest data rate that the access terminal associated with MACIndex 64-***n*** is allowed to use on the Reverse Traffic Channel, as shown in Table 8.5.6.3-1.

Table 8.5.6.3-1. Encoding of the RateLimit Field

Field value	Meaning
0x0	0 kbps
0x1	9.6 kbps
0x2	19.2 kbps
0x3	38.4 kbps
0x4	76.8 kbps
0x5	153.6 kbps
All other values	Invalid

Reserved — The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC	SLP	Best Effort
Addressing	broadcast	Priority	40

8.5.6.4 UnicastReverseRateLimit

The UnicastReverseRateLimit message is used by the access network to control the transmission rate on the reverse link for a particular access terminal.

Field	Length (bits)
MessageID	8
RateLimit	4
Reserved	4

MessageID — The access network shall set this field to 0x02.

RateLimit — The access network shall set this field to the highest data rate that the access terminal is allowed to use on the Reverse Traffic Channel, as shown in Table 8.5.6.4-1.

Table 8.5.6.4-1. Encoding of the RateLimit Field

Field value	Meaning
0x0	0 kbps
0x1	9.6 kbps
0x2	19.2 kbps
0x3	38.4 kbps
0x4	76.8 kbps
0x5	153.6 kbps
All other values	Invalid

Reserved — The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

Channels	CC FTC	SLP	Reliable
Addressing	unicast	Priority	40

8.5.6.5 Configuration Messages

The Default Reverse Traffic Channel MAC Protocol uses the Generic Configuration Protocol to transmit configuration parameters from the access network to the access terminal.

8.5.6.5.1 Configurable Attributes

The following configurable attributes are defined:

8.5.6.5.1.1 PowerParameters Attribute

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
DataOffsetNom	4	0
DataOffset9k6	4	0
DataOffset19k2	4	0
DataOffset38k4	4	0
DataOffset76k8	4	0
DataOffset153k6	4	0
RPCStep	2	1
Reserved	2	N/A

Length — Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — The access network shall set this field to 0x00.

ValueID — The access network shall set this field to an identifier assigned to this complex value.

DataOffsetNom — The access network shall set this field to the nominal offset of the reverse link data channel power to pilot channel power, expressed as 2's complement value in units of 0.5 dB. The access terminal shall support all the valid values specified by this field.

DataOffset9k6 — The access network shall set this field to the ratio of reverse link data channel power at 9.6 kbps to the nominal reverse link data channel power at9.6 kbps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field.

DataOffset19k2 — The access network shall set this field to the ratio of reverse link data channel power at 19.2 kbps to the nominal reverse link data channel power at 19.2 kbps, expressed as 2's complement in units of

0.25 dB. The access terminal shall support all the valid values specified by this field.

DataOffset38k4 — The access network shall set this field to the ratio of reverse link data channel power at 38.4 kbps to the nominal reverse link data channel power at 38.4 kbps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field.

DataOffset76k8 — The access network shall set this field to the ratio of reverse link data channel power at 76.8 kbps to the nominal reverse link data channel power at 76.8 kbps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field.

DataOffset153k6 — The access network shall set this field to the ratio of reverse link data channel power at 153.6 kbps to the nominal reverse link data channel power at 153.6 kbps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field.

RPCStep — Reverse Power Control step. The access network shall set this field to the power control step size the access terminal shall use when controlling the power of the reverse link, as shown in Table 8.5.6.5.1.1-1. The access terminal shall support all the valid values specified by this field.

Table 8.5.6.5.1.1-1. Encoding of the RPCStep Field

Field value (binary)	Meaning
'00'	0.5 dB
'01'	1.0 dB
All other values	Invalid

Reserved — The access network shall set this field to zero. The access terminal shall ignore this field.

8.5.6.5.1.2 RateParameters Attribute

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
Transition009k6_019k2	4	0xB
Transition019k2_038k4	4	0x4
Transition038k4_076k8	4	0x2
Transition076k8_153k6	4	0x2
Transition019k2_009k6	4	0x4
Transition038k4_019k2	4	0x4
Transition076k8_038k4	4	0x8
Transition153k6_076k8	4	0xF

Length — Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.

AttributeID — The access network shall set this field to 0x01.

ValueID — The access network shall set this field to an identifier assigned to this complex value.

Transition009k6_019k2

The field is set to indicate the probability the access terminal shall use to increase its transmission rate if its current transmission rate is 9.6 kbps. SeeTable 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition019k2_038k4

The field is set to indicate the probability the access terminal shall use to increase its transmission rate if its current transmission rate is 19.2 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition038k4_076k8

The field is set to indicate the probability the access terminal shall use to increase its transmission rate if its current transmission rate is 38.4 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition076k8_153k6

The field is set to indicate the probability the access terminal shall use to increase its transmission rate if its current transmission rate is 76.8 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition019k2_009k6

The field is set to indicate the probability the access terminal shall use to decrease its transmission rate if its current transmission rate is 19.2 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition038k4_019k2

The field is set to indicate the probability the access terminal shall use to decrease its transmission rate if its current transmission rate is 38.4 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition076k8_038k4

The field is set to indicate the probability the access terminal shall use to decrease its transmission rate if its current transmission rate is 76.8 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Transition153k6_076k8

The field is set to indicate the probability the access terminal shall use to decrease its transmission rate if its current transmission rate is 153.6 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with each value of the field. The access terminal shall support all the valid values specified by this field.

Table 8.5.6.5.1.2-1. Probability Table for the RateParameters Attribute

Value	Probability
0x0	0.0000
0x1	0.0625
0x2	0.1250
0x3	0.1875
0x4	0.2500
0x5	0.3125
0x6	0.3750
0x7	0.4375
0x8	0.5000
0x9	0.6250
0xA	0.6875
0xB	0.7500
0xC	0.8125
0xD	0.8750
0xE	0.9375
0xF	1.0000

8.5.6.5.2 ConfigurationRequest

The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x50.

Channels	CC FTC
Addressing	unicast

SLP	Reliable
Priority	40

8.5.6.5.3 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the access terminal includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response, and shall set the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

Channels	RTC
Addressing	unicast

SLP	Reliable
Priority	40

8.5.7 Protocol Numeric Constants

Constant	Meaning	Value
$N_{RTCMPType}$	Type field for this protocol	Table 2.3.6-1
$N_{RTCMPDefault}$	Subtype field for this protocol	0x0000
$T_{RTCMPATSetup}$	Maximum time for the access terminal to transmit the Reverse Traffic Channel in the Setup State	1.5 seconds
$T_{RTCMPANSetup}$	Maximum time for the access network to acquire the Reverse Traffic Channel and send a notification to the access terminal.	1 second

8.5.8 Interface to Other Protocols

8.5.8.1 Commands Sent

This protocol does not issue any commands.

8.5.8.2 Indications

This protocol does not register to receive any indications.

No text.

9 PHYSICAL LAYER

9.1 Physical Layer Packets

9.1.1 Overview

The transmission unit of the physical layer is a physical layer packet. A physical layer packet can be of length 256, 512, 1024, 2048, 3072, or 4096 bits. The format of the physical layer packet depends upon which channel it is transmitted on. A physical layer packet carries one or more MAC layer packets.

9.1.2 Physical Layer Packet Formats

9.1.2.1 Control Channel Physical Layer Packet Format

The length of a Control Channel physical layer packet shall be 1024 bits. Each Control Channel physical layer packet shall carry one Control Channel MAC layer packet. Control Channel physical layer packets shall use the following format:

Field	Length (bits)
MAC Layer Packet	1,002
FCS	16
TAIL	6

MAC Layer Packet - MAC layer packet from the Control Channel MAC protocol.

FCS - Frame check sequence (see 9.1.4).

TAIL - Encoder tail bits. This field shall be set to all '0's.

Figure 9.1.2.1-1 illustrates the format of the Control Channel physical layer packets.

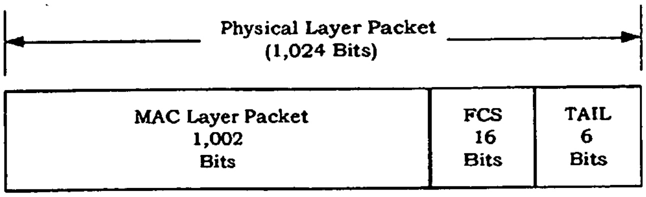


Figure 9.1.2.1-1. Physical Layer Packet Format for the Control Channel

9.1.2.2 Access Channel Physical Layer Packet Format

The length of an Access Channel physical layer packet shall be 256 bits. Each Access Channel physical layer packet shall carry one Access Channel MAC layer packet. Access Channel physical layer packets shall use the following format:

Field	Length (bits)
MAC Layer Packet	234
FCS	16
TAIL	6

MAC Layer Packet - MAC layer packet from the Access Channel MAC protocol.

FCS - Frame check sequence (see 9.1.4).

TAIL - Encoder tail bits. This field shall be set to all '0's.

Figure 9.1.2.2-1 illustrates the format of the Access Channel physical layer packets.

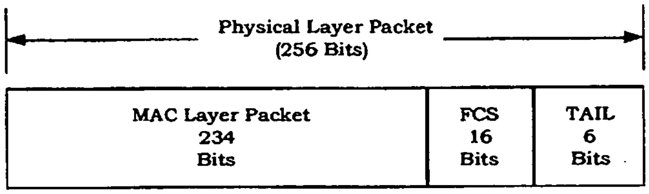


Figure 9.1.2.2-1. Physical Layer Packet Format for the Access Channel

9.1.2.3 Forward Traffic Channel Physical Layer Packet Format

The length of a Forward Traffic Channel physical layer packet shall be 1024, 2048, 3072, or 4096 bits. A Forward Traffic Channel physical layer packet shall carry 1, 2, 3, or 4 Forward Traffic Channel MAC layer packets depending on the rate of transmission. Forward Traffic Channel physical layer packets shall use the following format:

Field	Length (bits)
0, 1, 2, or 3 occurrences of the following two fields:	
MAC Layer Packet	1,002
PAD	22
One occurrence of the following three fields:	
MAC Layer Packet	1,002
FCS	16
TAIL	6

MAC Layer Packet - MAC layer packet from the Forward Traffic Channel MAC Protocol.

PAD - This field shall be set to all '0's. The receiver shall ignore this field.

FCS - Frame check sequence (see 9.1.4).

TAIL - Encoder tail bits. This field shall be set to all '0's.

Figure 9.1.2.3-1 illustrates the format of the Forward Traffic Channel physical layer packets.

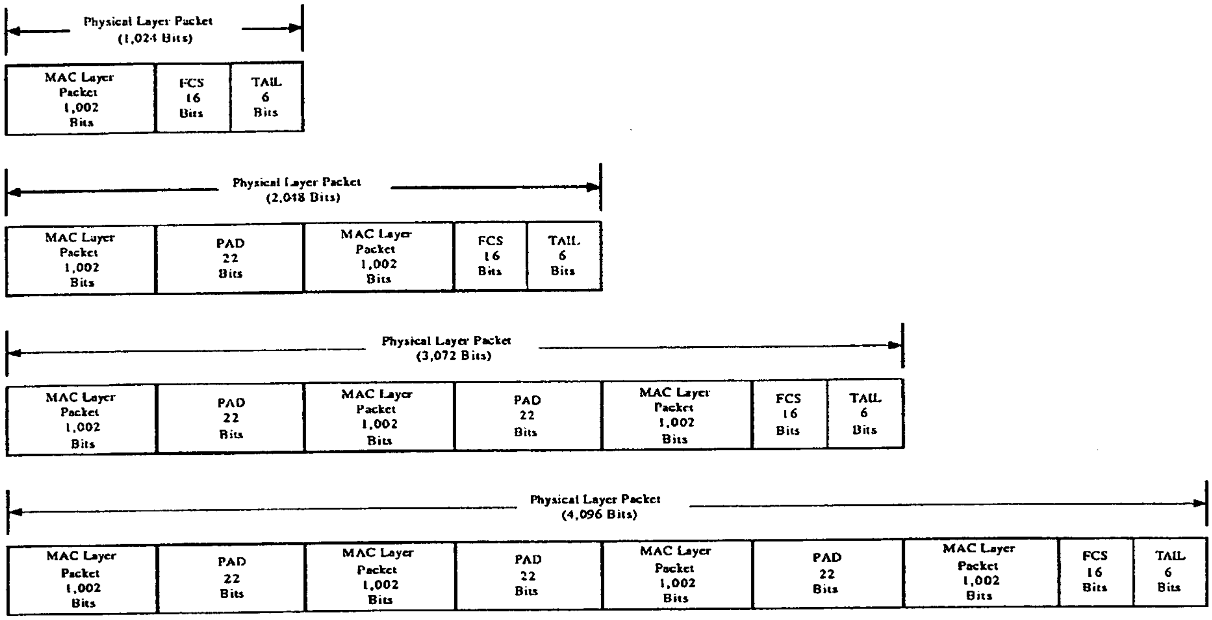

Physical Layer Packet (1,024 Bits)
MAC Layer Packet 1,002 Bits
FCS 16 Bits
TAIL 6 Bits
Physical Layer Packet (2,048 Bits)
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
FCS 16 Bits
TAIL 6 Bits
Physical Layer Packet (3,072 Bits)
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
FCS 16 Bits
TAIL 6 Bits
Physical Layer Packet (4,096 Bits)
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
PAD 22 Bits
MAC Layer Packet 1,002 Bits
FCS 16 Bits
TAIL 6 Bits

Figure 9.1.2.3-1. Physical Layer Packet Format for the Forward Traffic Channel

9.1.2.4 Reverse Traffic Channel Physical Layer Packet Format

The length of a Reverse Traffic Channel physical layer packet shall be 256, 512, 1024, 2048, or 4096 bits. Each Reverse Traffic Channel physical layer packet shall carry one Reverse Traffic Channel MAC layer packet. Reverse Traffic Channel physical layer packets shall use the following format:

Field	Length (bits)
MAC Layer Packet	234, 490, 1002, 2026, or 4074
FCS	16
TAIL	6

MAC Layer Packet - MAC layer packet from the Reverse Traffic Channel MAC Protocol.

FCS - Frame check sequence (see 9.1.4).

TAIL - Encoder tail bits. This field shall be set to all '0's.

Figure 9.1.2.4-1 illustrates the format of the Reverse Traffic Channel physical layer packets.

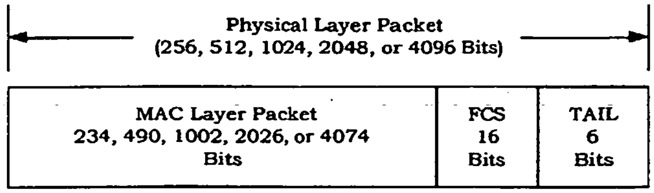

Physical Layer Packet
(256, 512, 1024, 2048, or 4096 Bits)
MAC Layer Packet
234, 490, 1002, 2026, or 4074
Bits
FCS
16
Bits
TAIL
6
Bits

Figure 9.1.2.4-1. Physical Layer Packet Format for the Reverse Traffic Channel

9.1.3 Bit Transmission Order

Each field of the physical layer packets shall be transmitted in sequence such that the most significant bit (MSB) is transmitted first and the least significant bit (LSB) is transmitted last. The MSB is the left-most bit in the figures of the document.

9.1.4 Computation of the FCS Bits

The FCS computation described here shall be used for computing the FCS field in the Control Channel physical layer packets, the Forward Traffic Channel physical layer packets, the Access Channel physical layer packets, and the Reverse Traffic Channel physical layer packets.

The FCS shall be a CRC calculated using the standard CRC-CCITT generator polynomial:

$$g(x) = x^{16} + x^{12} + x^{5} + 1.$$

The FCS shall be equal to the value computed according to the following procedure as shown in Figure 9.1.4-1:

?-? All shift-register elements shall be initialized to '0's.

?-? The switches shall be set in the up position.

?-? The register shall be clocked once for each bit of the physical layer packet except for the FCS and TAIL fields. The physical layer packet shall be read from MSB to LSB.

?-? The switches shall be set in the down position so that the output is a modulo-2 addition with a '0' and the successive shift-register inputs are '0's.

?-? The register shall be clocked an additional 16 times for the 16 FCS bits.

?-? The output bits constitute all fields of the physical layer packets except the TAIL field.

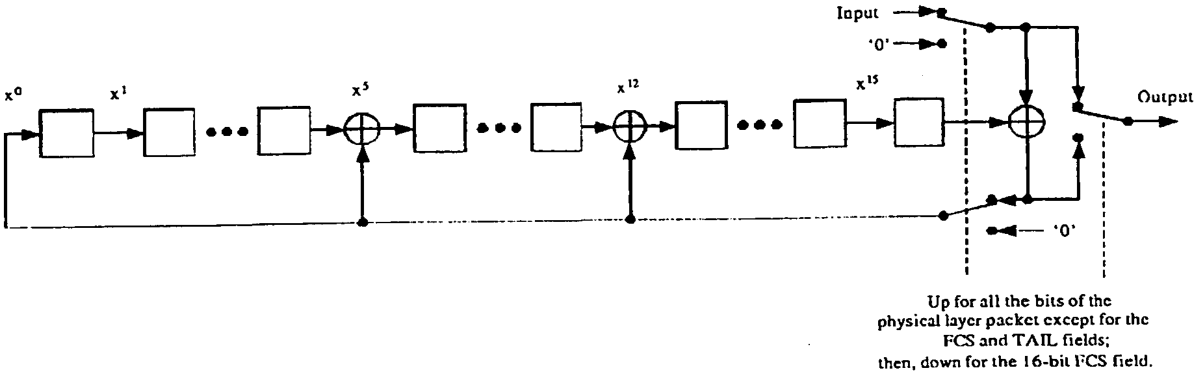

Input
'0'
x^0
x^1
x^5
x^{12}
x^{15}
Output
'0'
Up for all the bits of the physical layer packet except for the FCS and TAIL fields; then, down for the 16-bit FCS field.

Figure 9.1.4-1. FCS Computation for the Physical Layer Packet

9.2 Access Terminal Requirements

This section defines requirements specific to access terminal equipment and operation.

9.2.1 Transmitter

9.2.1.1 Frequency Parameters

9.2.1.1.1 Channel Spacing and Designation

9.2.1.1.1.1 Band Class 0 (800-MHz Band)

The Band Class 0 system designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.1-1.

There are two band subclasses specified for Band Class 0. Access terminals supporting Band Class 0 shall support at least one band subclass belonging to Band Class 0.

Access terminals supporting Band Class 0 shall be capable of transmitting in Band Class 0.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 0 shall be as specified in Table 9.2.1.1.1.1-2. Access terminals supporting Band Class 0 shall support transmission on the valid channel numbers shown in Table 9.2.1.1.1.1-3.[41]

The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.1-1. Band Class 0 System Frequency Correspondence

System Designator	Band Subclass	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
A	0	824.025–835.005 844.995–846.495	869.025–880.005 889.995–891.495
	1	824.025–835.005 844.995–848.985	869.025–880.005 889.995–893.985
B	0	835.005–844.995 846.495–848.985	880.005–889.995 891.495–893.985
	1	835.005–844.995	880.005–889.995

[41] Note that the Korean Cellular Band uses Band Subclass 1 and has additional valid channels that a Band Class 0 access terminal should support to permit roaming to Korea.

Table 9.2.1.1.1.1-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 0

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	1 = N = 799	0.030 N + 825.000
	991 = N = 1023	0.030 (N – 1023) + 825.000
Access Network	1 = N = 799	0.030 N + 870.000
	991 = N = 1023	0.030 (N – 1023) + 870.000

Table 9.2.1.1.1.1-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 0

Band Subclass	System Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
				Access Terminal	Access Network
0	A"	Not Valid	991–1012	824.040–824.670	869.040–869.670
	(1 MHz)	Valid	1013–1023	824.700–825.000	869.700–870.000
	A	Valid	1–311	825.030–834.330	870.030–879.330
	(10 MHz)	Not Valid	312–333	834.360–834.990	879.360–879.990
	B	Not Valid	334–355	835.020–835.650	880.020–880.650
	(10 MHz)	Valid	356–644	835.680–844.320	880.680–889.320
		Not Valid	645–666	844.350–844.980	889.350–889.980
	A'	Not Valid	667–688	845.010–845.640	890.010–890.640
	(1.5 MHz)	Valid	689–694	845.670–845.820	890.670–890.820
		Not Valid	695–716	845.850–846.480	890.850–891.480
	B'	Not Valid	717–738	846.510–847.140	891.510–892.140
	(2.5 MHz)	Valid	739–777	847.170–848.310	892.170–893.310
		Not Valid	778–799	848.340–848.970	893.340–893.970
1	A"	Not Valid	991–1012	824.040–824.670	869.040–869.670
	(1 MHz)	Valid	1013–1023	824.700–825.000	869.700–870.000
	A	Valid	1–311	825.030–834.330	870.030–879.330
	(10 MHz)	Not Valid	312–333	834.360–834.990	879.360–879.990
	B	Not Valid	334–355	835.020–835.650	880.020–880.650
	(10 MHz)	Valid	356–644	835.680–844.320	880.680–889.320
		Not Valid	645–666	844.350–844.980	889.350–889.980
	A'	Not Valid	667–688	845.010–845.640	890.010–890.640
	(1.5 MHz)	Valid	689–716	845.670–846.480	890.670–891.480
	A'''	Valid	717–779	846.510–848.370	891.510–893.370
	(2.5 MHz)	Not Valid	780–799	848.400–848.970	893.400–893.970

9.2.1.1.1.2 Band Class 1 (1900-MHz Band)

The Band Class 1 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.2-1.

Access terminals supporting Band Class 1 shall be capable of transmitting in Band Class 1.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 1 shall be as specified in Table 9.2.1.1.1.2-2. Access terminals supporting Band Class 1 shall support transmission on the valid and conditionally valid channel numbers shown in Table 9.2.1.1.1.2-3. Note that certain channel assignments are not valid and others are conditionally valid. Transmission on conditionally valid channels is permissible if the adjacent block is allocated to the same licensee or if other valid authorization has been obtained.

The nominal access terminal transmit carrier frequency shall be 80.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.2-1. Band Class 1 Block Frequency Correspondence

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	1850–1865	1930–1945
D	1865–1870	1945–1950
B	1870–1885	1950–1965
E	1885–1890	1965–1970
F	1890–1895	1970–1975
C	1895–1910	1975–1990

Table 9.2.1.1.1.2-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 1

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 1199	1850.000 + 0.050 N
Access Network	0 = N = 1199	1930.000 + 0.050 N

Table 9.2.1.1.1.2-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 1

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (15 MHz)	Not Valid	0–24	1850.000–1851.200	1930.000–1931.200
	Valid	25–275	1851.250–1863.750	1931.250–1943.750
	Cond. Valid	276–299	1863.800–1864.950	1943.800–1944.950
D (5 MHz)	Cond. Valid	300–324	1865.000–1866.200	1945.000–1946.200
	Valid	325–375	1866.250–1868.750	1946.250–1948.750
	Cond. Valid	376–399	1868.800–1869.950	1948.800–1949.950
B (15 MHz)	Cond. Valid	400–424	1870.000–1871.200	1950.000–1951.200
	Valid	425–675	1871.250–1883.750	1951.250–1963.750
	Cond. Valid	676–699	1883.800–1884.950	1963.800–1964.950
E (5 MHz)	Cond. Valid	700–724	1885.000–1886.200	1965.000–1966.200
	Valid	725–775	1886.250–1888.750	1966.250–1968.750
	Cond. Valid	776–799	1888.800–1889.950	1968.800–1969.950
F (5 MHz)	Cond. Valid	800–824	1890.000–1891.200	1970.000–1971.200
	Valid	825–875	1891.250–1893.750	1971.250–1973.750
	Cond. Valid	876–899	1893.800–1894.950	1973.800–1974.950
C (15 MHz)	Cond. Valid	900–924	1895.000–1896.200	1975.000–1976.200
	Valid	925–1175	1896.250–1908.750	1976.250–1988.750
	Not Valid	1176–1199	1908.800–1909.950	1988.800–1989.950

9.2.1.1.1.3 Band Class 2 (TACS Band)

The Band Class 2 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.3-1.

Access terminals supporting Band Class 2 shall be capable of transmitting in Band Class 2 using at least one band subclass. The band subclasses for Band Class 2 are specified in Table 9.2.1.1.1.3-2.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 2 shall be as specified in Table 9.2.1.1.1.3-3. Access terminals supporting Band Class 2 shall support transmission on the valid and conditionally valid channel numbers shown in Table 9.2.1.1.1.3-4. Transmission on the conditionally valid channels is permissible if valid authorization has been obtained.

The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.3-1. Band Class 2 Block Frequency Correspondence

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	872.0125–879.9875 890.0125–897.4875 905.0125–908.9875	917.0125–924.9875 935.0125–942.4875 950.0125–953.9875
B	880.0125–887.9875 897.5125–904.9875 909.0125–914.9875	925.0125–932.9875 942.5125–949.9875 954.0125–959.9875

Table 9.2.1.1.1.3-2. Band Class 2 Band Subclasses

Band Subclass	Number of Channels Covered	Channels Covered
0	600	1–600
1	1000	1–1000
2	1320	1329–2047 and 0–600

Table 9.2.1.1.1.3-3. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 2

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 1000	0.025 N + 889.9875
	1329 = N = 2047	0.025 (N – 1328) + 871.9875
Access Network	0 = N = 1000	0.025 N + 934.9875
	1329 = N = 2047	0.025 (N – 1328) + 916.9875

Table 9.2.1.1.1.3-4. CDMA Channel Numbers and Corresponding Frequencies for Band Class 2

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A ETACS (8 MHz)	Not Valid Valid-1320	1329–1355 1356–1648	872.0125–872.6625 872.6875–879.9875	917.0125–917.6625 917.6875–924.9875
B ETACS (8 MHz)	Valid-1320 Cond. Valid-1320	1649–1941 1942–1968	880.0125–887.3125 887.3375–887.9875	925.0125–932.3125 932.3375–932.9875
Unassigne d (2 MHz)	Cond. Valid-1320	1969–2047 0	888.0125–889.9625 889.9875	933.0125–934.9625 934.9875
A (7.5 MHz)	Cond. Valid-1320 Valid	1–27 28–300	890.0125–890.6625 890.6875–897.4875	935.0125–935.6625 935.6875–942.4875
B (7.5 MHz)	Valid Valid-1000	301–573 574–600	897.5125–904.3125 904.3375–904.9875	942.5125–949.3125 949.3375–949.9875
A′ (4 MHz)	Valid-1000	601–760	905.0125–908.9875	950.0125–953.9875
B′ (6 MHz)	Valid-1000 Not Valid	761–973 974–1000	909.0125–914.3125 914.3375–914.9875	954.0125–959.3125 959.3375–959.9875

Valid and Not Valid apply to the channels for the access terminals of all three band subclasses. Valid-1000 means that the channels are only valid for the access terminals of band subclass 1. Valid-1320 means that the channels are only valid for the access terminals of band subclass 2. Cond. Valid-1320 means that the channels are conditionally valid for the access terminals of band subclass 2, and that they are not valid for the access terminals of band subclasses 0 and 1.

9.2.1.1.1.4 Band Class 3 (JTACS Band)

The Band Class 3 system designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.4-1.

Access terminals supporting Band Class 3 shall be capable of transmitting in Band Class 3.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 3 shall be as specified in Table 9.2.1.1.1.4-2. Access terminals supporting Band Class 3 shall support transmission on the valid channel numbers shown in Table 9.2.1.1.1.4-3.

The nominal access terminal transmit carrier frequency shall be 55.0 MHz higher than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.4-1. Band Class 3 System Frequency Correspondence

System Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	887.0125–888.9875 893.0125–898.0000 898.0125–900.9875 915.0125–924.9875	832.0125–833.9875 838.0125–843.0000 843.0125–845.9875 860.0125–869.9875
B	Not specified	Not specified

Table 9.2.1.1.1.4-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 3

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	1 = N = 799	0.0125 N + 915.000
	801 = N = 1039	0.0125 (N – 800) + 898.000
	1041 = N = 1199	0.0125 (N – 1040) + 887.000
	1201 = N = 1600	0.0125 (N – 1200) + 893.000
Access Network	1 = N = 799	0.0125 N + 860.000
	801 = N = 1039	0.0125 (N – 800) + 843.000
	1041 = N = 1199	0.0125 (N – 1040) + 832.000
	1201 = N = 1600	0.0125 (N – 1200) + 838.000

In this table, only even-valued N values are valid.

Table 9.2.1.1.1.4-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 3

System Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A1 (2 MHz)	Not Valid Valid Not Valid	1041–1099 1100–1140 1141–1199	887.0125–887.7375 887.7500–888.2500 888.2625–888.9875	832.0125–832.7375 832.7500–833.2500 833.2625–833.9875
A3 (5 MHz)	Not Valid Valid Cond. Valid	1201–1259 1260–1540 1541–1600	893.0125–893.7375 893.7500–897.2500 897.2625–898.0000	838.0125–838.7375 838.7500–842.2500 842.2625–843.0000
A2 (3 MHz)	Cond. Valid Valid Not Valid	801–859 860–980 981–1039	898.0125–898.7375 898.7500–900.2500 900.2625–900.9875	843.0125–843.7375 843.7500–845.2500 845.2625–845.9875
A (10 MHz)	Not Valid Valid Not Valid	1–59 60–740 741–799	915.0125–915.7375 915.7500–924.2500 924.2625–924.9875	860.0125–860.7375 860.7500–869.2500 869.2625–869.9875
B	Not specified	Not specified	Not specified	Not specified

9.2.1.1.1.5 Band Class 4 (Korean PCS Band)

The Band Class 4 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.5-1.

Access terminals supporting Band Class 4 shall be capable of transmitting in Band Class 4.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 4 shall be as specified in Table 9.2.1.1.1.5-2. Access terminals supporting Band Class 4 shall support transmission on the valid and conditionally valid channel numbers shown in Table 9.2.1.1.1.5-3. Transmission on conditionally valid channels is permissible if the adjacent block is allocated to the same licensee or if other valid authorization has been obtained.

The nominal access terminal transmit carrier frequency shall be 90.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.5-1. Band Class 4 Block Frequency Correspondence

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	1750–1760	1840–1850
B	1760–1770	1850–1860
C	1770–1780	1860–1870

Table 9.2.1.1.1.5-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 4

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 599	0.050 N + 1750.000
Access Network	0 = N = 599	0.050 N + 1840.000

Table 9.2.1.1.1.5-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 4

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (10 MHz)	Not Valid Valid Cond. Valid	0–24 25–175 176–199	1750.000–1751.200 1751.250–1758.750 1758.800–1759.950	1840.000–1841.200 1841.250–1848.750 1848.800–1849.950
B (10 MHz)	Cond. Valid Valid Cond. Valid	200–224 225–375 376–399	1760.000–1761.200 1761.250–1768.750 1768.800–1769.950	1850.000–1851.200 1851.250–1858.750 1858.800–1859.950
C (10 MHz)	Cond. Valid Valid Not Valid	400–424 425–575 576–599	1770.000–1771.200 1771.250–1778.750 1778.800–1779.950	1860.000–1861.200 1861.250–1868.750 1868.800–1869.950

9.2.1.1.1.6 Band Class 5 (450-MHz Band)

The Band Class 5 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.6-1.

There are eight band subclasses specified for Band Class 5. Each band subclass corresponds to a specific block designator (see Table 9.2.1.1.1.6-1). Each band subclass includes all the channels designated for that system. Access terminals supporting Band Class 5 shall be capable of transmitting in at least one band subclass belonging to Band

Class 5. For access terminals capable of transmitting in more than one band subclass belonging to Band Class 5, one band subclass shall be designated as the Primary Band Subclass, which is the band subclass used by the access terminal's home system.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 5 shall be as specified in Table 9.2.1.1.1.6-2. Access terminals supporting Band Class 5 shall support transmission on the valid and conditionally valid channel numbers shown in Table 9.2.1.1.1.6-3, depending on the Band Subclass of the access terminal. Note that certain channel assignments in Block A are not valid and others are conditionally valid. Transmission on conditionally valid channels is permissible if the adjacent A' block is allocated to the same licensee or if other valid authorization has been obtained.

The nominal access terminal transmit carrier frequency shall be 10.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.6-1. Band Class 5 Block Frequency Correspondence and Band Subclasses

Block Designator	Band Subclass	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
A	0	452.500–457.475	462.500–467.475
B	1	452.000–456.475	462.000–466.475
C	2	450.000–454.800	460.000–464.800
D	3	411.675–415.850	421.675–425.850
E	4	415.500–419.975	425.500–429.975
F	5	479.000–483.480	489.000–493.480
G	6	455.230–459.990	465.230–469.990
H	7	451.310–455.730	461.310–465.730

Table 9.2.1.1.1.6-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 5

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	1 = N = 300	0.025 (N – 1) + 450.000
	539 = N = 871	0.025 (N – 512) + 411.000
	1039 = N = 1473	0.020 (N – 1024) + 451.010
	1792 = N = 2016	0.020 (N – 1792) + 479.000
Access Network	1 = N = 300	0.025 (N – 1) + 460.000
	539 = N = 871	0.025 (N – 512) + 421.000
	1039 = N = 1473	0.020 (N – 1024) + 461.010
	1792 = N = 2016	0.020 (N – 1792) + 489.000

Table 9.2.1.1.1.6-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 5

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (4.5 MHz)	Not Valid	121–125	453.000–453.100	463.000–463.100
	Cond. Valid	126–145	453.125–453.600	463.125–463.600
	Valid	146–275	453.625–456.850	463.625–466.850
	Not Valid	276–300	456.875–457.475	466.875–467.475
A′ (0.5 MHz)	Not Valid	101–120	452.500–452.975	462.500–462.975
B (4.5 MHz)	Not Valid	81–105	452.000–452.600	462.000–462.600
	Valid	106–235	452.625–455.850	462.625–465.850
	Not Valid	236–260	455.875–456.475	465.875–466.475
C (4.8 MHz)	Not Valid	1–25	450.000–450.600	460.000–460.600
	Valid	26–168	450.625–454.175	460.625–464.175
	Not Valid	169–193	454.200–454.800	464.200–464.800
D (4.2 MHz)	Not Valid	539–563	411.675–412.275	421.675–422.275
	Valid	564–681	412.300–415.225	422.300–425.225
	Not Valid	682–706	415.250–415.850	425.250–425.850
E (4.5 MHz)	Not Valid	692–716	415.500–416.100	425.500–426.100
	Valid	717–846	416.125–419.350	426.125–429.350
	Not Valid	847–871	419.375–419.975	429.375–429.975
F (4.5 MHz)	Not Valid	1792–1822	479.000–479.600	489.000–489.600
	Valid	1823–1985	479.620–482.860	489.620–492.860
	Not Valid	1986–2016	482.880–483.480	492.880–493.480
G (4.76 MHz)	Not Valid	1235–1265	455.230–455.830	465.230–465.830
	Valid	1266–1442	455.850–459.370	465.850–469.370
	Not Valid	1443–1473	459.390–459.990	469.390–469.990
H (4.42 MHz)	Not Valid	1039–1069	451.310–451.910	461.310–461.910
	Valid	1070–1229	451.930–455.110	461.930–465.110
	Not Valid	1230–1260	455.130–455.730	465.130–465.730

9.2.1.1.1.7 Band Class 6 (2-GHz Band)

The Band Class 6 block designators for the access terminal and access network are not specified, since licensee allocations vary by regulatory body.

Access terminals supporting Band Class 6 shall be capable of transmitting in Band Class 6.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 6 shall be as specified in Table 9.2.1.1.1.7-1. Access terminals supporting Band

Class 6 shall support transmission on the valid channel numbers shown in Table 9.2.1.1.1.7-2.

The nominal access terminal transmit carrier frequency shall be 190.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.7-1. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 6

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 1199	1920.000 + 0.050 N
Access Network	0 = N = 1199	2110.000 + 0.050 N

Table 9.2.1.1.1.7-2. CDMA Channel Numbers and Corresponding Frequencies for Band Class 6

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	1920.000–1921.200	2110.000–2111.200
Valid	25–1175	1921.250–1978.750	2111.250–2168.750
Not Valid	1176–1199	1978.800–1979.950	2168.800–2169.950

Channel numbers less than 1.25 MHz from the licensee's band edge are not valid.

9.2.1.1.1.8 Band Class 7 (700-MHz Band)

The Band Class 7 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.1.8-1.

Access terminals supporting Band Class 7 shall be capable of transmitting in Band Class 7.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 7 shall be as specified in Table 9.2.1.1.1.8-2. Access terminals supporting Band Class 7 shall support operations on the valid and conditionally valid channel numbers shown in Table 9.2.1.1.1.8-3. Note that certain channel assignments are not valid and others are conditionally valid. Transmission on conditionally valid channels is permissible if the adjacent block is allocated to the same licensee or if other valid authorization has been obtained.

The nominal access terminal transmit carrier frequency shall be 30.0 MHz higher than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.8-1. Band Class 7 Block Frequency Correspondence

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	776–777	746–747
C	777–782	747–752
D	782–792	752–762
B	792–794	762–764

Table 9.2.1.1.1.8-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 7

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 359	776.000 + 0.050 N
Access Network	0 = N = 359	746.000 + 0.050 N

Table 9.2.1.1.1.8-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 7

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (1 MHz)	Not Valid	0–19	776.000–776.950	746.000–746.950
C (5 MHz)	Not Valid Valid Cond. Valid	20–44 45–95 96–119	777.000–778.200 778.250–780.750 780.800–781.950	747.000–748.200 748.250–750.750 750.800–751.950
D (10 MHz)	Cond. Valid Valid Not Valid	120–144 145–295 296–319	782.000–783.200 783.250–790.750 790.800–791.950	752.000–753.200 753.250–760.750 760.800–761.950
B (2 MHz)	Not Valid	320–359	792.000–793.950	762.000–763.950

9.2.1.1.1.9 Band Class 8 (1800-MHz Band)

The Band Class 8 block designators for the access terminal and the access network are not specified.

Access terminals supporting Band Class 8 shall be capable of transmitting in Band Class 8.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 8 shall be as specified in Table 9.2.1.1.1.9-1. Access terminals supporting Band Class 8 shall support transmission on the valid channel numbers shown in Table 9.2.1.1.1.9-2.

The nominal access terminal transmit carrier frequency shall be 95.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.9-1. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 8

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 1499	1710.000 + 0.050 N
Access Network	0 = N = 1499	1805.000 + 0.050 N

Table 9.2.1.1.1.9-2. CDMA Channel Numbers and Corresponding Frequencies for Band Class 8

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	1710.000–1711.200	1805.000-1806.200
Valid	25–1475	1711.250-1783.750	1806.250-1878.750
Not Valid	1476–1499	1783.800-1784.950	1878.800-1879.950

Channel numbers less than 1.25 MHz from the licensee's band edge are not valid.

9.2.1.1.1.10 Band Class 9 (900-MHz Band)

The Band Class 9 block designators for the access terminal and the access network are not specified.

Access terminals supporting Band Class 9 shall be capable of transmitting in Band Class 9.

The channel spacing, CDMA channel designations, and transmitter center frequencies of Band Class 9 shall be as specified in Table 9.2.1.1.1.10-1. Access terminals supporting Band Class 9 shall support transmission on the valid channel numbers shown Table 9.2.1.1.1.10-2.

The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the frequency of the access network transmit signal as measured at the access terminal receiver.

Table 9.2.1.1.1.10-1. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 9

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	0 = N = 699	880.000 + 0.050 N
Access Network	0 = N = 699	925.000 + 0.050 N

Table 9.2.1.1.1.10-2. CDMA Channel Numbers and Corresponding Frequencies for Band Class 9

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	880.000–881.200	925.000-926.200
Valid	25–675	881.250-913.750	926.250-958.750
Not Valid	676–699	913.800-914.950	958.800-959.950

Channel numbers less than 1.25 MHz from the licensee's band edge are not valid.

9.2.1.1.2 Frequency Tolerance

The access terminal shall meet the requirements in the current version of [5].

9.2.1.2 Power Output Characteristics

All power levels are referenced to the access terminal antenna connector unless otherwise specified.

9.2.1.2.1 Output Power Requirements of Reverse Channels

9.2.1.2.1.1 Access Channel Output Power

When transmitting over the Access Channel, the access terminal transmits Access Probes until the access attempt succeeds or ends.

9.2.1.2.1.2 Reverse Traffic Channel Output Power

When the access terminal is transmitting the Reverse Traffic Channel, the access terminal shall control the mean output power using a combination of closed-loop and open-loop power control (see 9.2.1.2.4 and 9.2.1.4). Throughout 9.2.1.2, the channel formed by multiplexing the RRI Channel onto the Pilot Channel is still referred to as the Pilot Channel.

When the access terminal is transmitting the Reverse Traffic Channel, the access terminal transmits the Pilot Channel, the DRC Channel, the ACK Channel when acknowledging received physical layer packets, and the Data Channel when transmitting physical layer packets. These channels shall be transmitted at power levels according to open-loop and closed-loop power control. The transmitted power level of the Data Channel shall be adjusted depending on the selected data rate (see 9.2.1.2.4) and reverse link power control. The traffic data shall be transmitted in the form of physical layer packets (duration 26.66... ms), which may occur either contiguously or sporadically. When the data rate is changed, the access terminal output power, relative to the desired value in steady state, shall be within ±0.5 dB or 20% of the change in dB, whichever is greater. The access terminal output power shall settle to within ±0.5 dB of the steady-state value within 200 μs of the physical layer packet boundary.

9.2.1.2.2 Maximum Output Power

The access terminal shall meet the requirements in the current version of [5].

9.2.1.2.3 Output Power Limits

9.2.1.2.3.1 Minimum Controlled Output Power

The access terminal shall meet the requirements in the current version of [5].

9.2.1.2.3.2 Standby Output Power

The access terminal shall disable its transmitter except when it is instructed by a MAC protocol to transmit. When the transmitter is disabled, the output noise power spectral density of the access terminal shall be less than −61 dBm/1 MHz for all frequencies within the transmit bands that the access terminal supports.

9.2.1.2.4 Controlled Output Power

The access terminal shall provide two independent means for output power adjustment: an open-loop estimation performed by the access terminal and a closed-loop correction involving both the access terminal and the access network. Accuracy requirements on the controlled range of mean output power (see 9.2.1.2.5) need not apply for the following three cases:

- Mean output power levels exceeding the minimum ERP/EIRP at the maximum output power for the corresponding access terminal class;
- Mean output power levels less than the minimum controlled output power (see 9.2.1.2.3.1); or
- Mean input power levels exceeding −25 dBm within the 1.23-MHz bandwidth.

9.2.1.2.4.1 Estimated Open-Loop Output Power

Open-loop operation shall be based on the power of the received Forward Pilot Channel (see 9.3.1.3.2.1).

The nominal access probe structure and its transmit power requirements are defined as part of the Access Channel MAC Protocol. The power of the Access Data Channel relative to that of the Pilot Channel shall be as specified in Table 9.2.1.2.4.1-1 in which DataOffsetNom and DataOffset9k6 are public data of the Access Channel MAC Protocol. The output power of the Pilot Channel during the preamble portion of an access probe shall be increased relative to the nominal Pilot Channel power during the data portion of the probe by an amount such that the total output power of the preamble and data portions of the access probe are the same.

Once instructed by the Reverse Traffic Channel MAC Protocol, the access terminal initiates Reverse Traffic Channel transmission. The initial mean output power of the Pilot Channel of the Reverse Traffic Channel shall be equal to the mean output power of the Pilot Channel at the end of the last Access Channel probe minus the difference in the forward link mean received signal power from the end of the last Access Channel probe to the start of the Reverse Traffic Channel transmission.

The subsequent mean output power of the Pilot Channel of the total reverse link transmission shall be as specified in 9.2.1.2.4.2.

The accuracy of the incremental adjustment to the mean output power, as dictated by the Access Channel MAC Protocol and the Reverse Traffic Channel MAC Protocol, shall be ±0.5 dB or 20% of the change (in dB), whichever is greater.

The access terminal shall support a total combined range of initial offset parameters, access probe corrections, and closed-loop power control corrections, of at least ±32 dB for access terminals operating in Band Classes 0, 2, 3, 5, and 7 and ±40 dB for access terminals operating in Band Classes 1, 4, and 6.

Prior to the application of access probe corrections and closed-loop power control corrections, the access terminal's open-loop mean output power of the Pilot Channel, X_0, should be within ±6 dB and shall be within ±9 dB of the value given by

$$X_0 = -\text{Mean Received Power (dBm)} + \text{OpenLoopAdjust} + \text{ProbeInitialAdjust}$$

where OpenLoopAdjust and ProbeInitialAdjust are public data from the Access Channel MAC Protocol and OpenLoopAdjust + ProbeInitialAdjust is from –81 to –66 dB for Band Classes 0, 2, 3, 5, and 7 and from –100 to –69 dB for Band Classes 1, 4, and 6.

During the transmission of the Reverse Traffic Channel, the determination of the output power needed to support the Data Channel, the DRC Channel, and the ACK Channel is an additional open-loop process performed by the access terminal.

The power of the Data Channel relative to that of the Pilot Channel shall be as specified in Table 9.2.1.2.4.1-1 in which DataOffsetNom, DataOffset9k6, DataOffset19k2, DataOffset38k4, DataOffset76k8, and DataOffset153k6 are public data of the Reverse Traffic Channel MAC Protocol.

Table 9.2.1.2.4.1-1. Relative Power Levels vs. Data Rate

Data Rate (kbps)	Data Channel Gain Relative to Pilot (dB)
0	–∞ (Data Channel Is Not Transmitted)
9.6	DataOffsetNom + DataOffset9k6 + 3.75
19.2	DataOffsetNom + DataOffset19k2 + 6.75
38.4	DataOffsetNom + DataOffset38k4 + 9.75
76.8	DataOffsetNom + DataOffset76k8 + 13.25
153.6	DataOffsetNom + DataOffset153k6 + 18.5

During the transmission of the DRC Channel, the power of the DRC Channel relative to that of the Pilot Channel shall be as specified by DRCChannelGain, where DRCChannelGain is public data of the Forward Traffic Channel MAC Protocol.

During the transmission of the ACK Channel, the power of the ACK Channel relative to that of the Pilot Channel shall be as specified by ACKChannelGain, where ACKChannelGain is public data of the Forward Traffic Channel MAC Protocol.

The access terminal shall maintain the power of the Data Channel, DRC Channel and ACK Channel, relative to that of the Pilot Channel, to within ±0.25 dB of the specified values.

If the access terminal is unable to transmit at the requested output power level when the maximum Reverse Traffic Channel data rate is 9600 bps, the access terminal shall reduce the power of the DRC Channel and the ACK Channel accordingly. The maximum power reduction for the DRC Channel corresponds to gating off the DRC Channel. The maximum power reduction for the ACK Channel corresponds to gating off the ACK Channel. If the ACK Channel is active, the ACK Channel power reduction shall occur only after the DRC Channel has been gated off. The access terminal shall perform the power reduction within one slot of determining that the access terminal is unable to transmit at the requested output power level.

9.2.1.2.4.2 Closed-Loop Output Power

For closed-loop correction (with respect to the open-loop estimate), the access terminal shall adjust the mean output power level of the Pilot Channel in response to each power-control bit received on the Reverse Power Control (RPC) Channel. The nominal change in mean output power level of the Pilot Channel per single power-control bit shall be set according to the RPCStep public data of the Reverse Traffic Channel MAC Protocol.

For the 1.0 dB step size, the change in mean output power level per power-control bit shall be within ±0.5 dB of the nominal value (1 dB), and the change in mean output power level per 10 power-control bits of the same sign shall be within ±2.0 dB of 10 times the nominal change (10 dB). For the 0.5 dB step size, the change in mean output power level per power-control bit shall be within ±0.3 dB of the nominal value (0.5 dB), and the change in mean output power level per 20 power-control bits of the same sign shall be within ±2.5 dB of 20 times the nominal change (10 dB). A '0' power-control bit requires the access terminal to increase transmit power, and a '1' power-control bit requires the access terminal to decrease transmit power. The access terminal shall provide a closed-loop adjustment range greater than ±24 dB around its open-loop estimate.

See 9.2.1.4 for combining power-control bits received from different multipath components or from different sectors during handoff.

9.2.1.2.5 Power Transition Characteristics

9.2.1.2.5.1 Open-Loop Estimation

Following a step change in mean input power, ΔP_{in}, the mean output power of the access terminal shall transition to its final value in a direction opposite in sign to ΔP_{in}, with magnitude contained between the mask limits defined by[42]:

- Upper Limit:

  For $0 < t < 24$ ms: $\max[1.2 \times |\Delta P_{in}| \times (t/24), |\Delta P_{in}| \times (t/24) + 2.0 \text{ dB}] + 1.5 \text{ dB}$

  For $t \geq 24$ ms: $\max[1.2 \times |\Delta P_{in}|, |\Delta P_{in}| + 0.5 \text{ dB}] + 1.5 \text{ dB}$

- Lower Limit:

  For $t > 0$: $\max[0.8 \times |\Delta P_{in}| \times [1 - e^{(1.66\ldots-t)/36}] - 2.0 \text{ dB}, 0] - 1 \text{ dB}$

where "t" is expressed in units of milliseconds and ΔP_{in} is expressed in units of dB.

These limits shall apply to a step change ΔP_{in} of ±20 dB or less. The absolute value of the change in mean output power due to open-loop power control shall be a monotonically increasing function of time. If the change in mean output power consists of discrete increments, no single increment shall exceed 1.2 dB.

9.2.1.2.5.2 Closed-Loop Correction

Following the reception of a closed-loop power-control bit, the mean output power of the access terminal shall be within 0.3 dB and 0.15 dB of the final value in less than 500 µs for step sizes of 1.0 dB and 0.5 dB, respectively.

9.2.1.3 Modulation Characteristics

9.2.1.3.1 Reverse Channel Structure

The Reverse Channel consists of the Access Channel and the Reverse Traffic Channel. The Access Channel shall consist of a Pilot Channel and a Data Channel. The Reverse Traffic Channel shall consist of a Pilot Channel, a Reverse Rate Indicator (RRI) Channel, a

[42] The mask limits allow for the effect of alternating closed-loop power-control bits.

Data Rate Control (DRC) Channel, an Acknowledgement (ACK) Channel, and a Data Channel. The RRI Channel is used to indicate the data rate of the Data Channel being transmitted on the Reverse Traffic Channel. The DRC Channel is used by the access terminal to indicate to the access network the requested Forward Traffic Channel data rate and the selected serving sector on the Forward Channel. The ACK Channel is used by the access terminal to inform the access network whether or not the physical layer packet transmitted on the Forward Traffic Channel has been received successfully.

The structure of the reverse link channels for the Access Channel shall be as shown in Figure 9.2.1.3.1-1, and the structure of the reverse link channels for the Reverse Traffic Channel shall be as shown in Figure 9.2.1.3.1-2 and Figure 9.2.1.3.1-3. For the Reverse Traffic Channel, the encoded RRI Channel symbols shall be time-division multiplexed with the Pilot Channel. This time-division-multiplexed channel is still referred to as the Pilot Channel. For the Access Channel, the RRI symbols shall not be transmitted and the Pilot Channel shall not be time-division multiplexed. The Pilot Channel, the DRC Channel, the ACK Channel, and the Data Channel shall be orthogonally spread by Walsh functions of length 4, 8, or 16 (see 9.2.1.3.7). Each Reverse Traffic Channel shall be identified by a distinct user long code. The Access Channel for each sector shall be identified by a distinct Access Channel long code.

The Access Channel frame and Reverse Traffic Channel frame shall be 26.66... ms in duration and the frame boundary shall be aligned to the rollover of the short PN codes (see 9.2.1.3.8.1). Each frame shall consist of 16 slots, with each slot 1.66... ms in duration. Each slot contains 2048 PN chips.

When the access terminal is transmitting a Reverse Traffic Channel, it shall continuously transmit the Pilot Channel and the RRI Channel. These channels shall be time-division multiplexed, and shall be transmitted on Walsh channel W_0^{16}. When the DRC Channel is active (see 9.2.1.3.3.3), it shall be transmitted for full slot durations on Walsh channel W_8^{16}. The access terminal shall transmit an ACK Channel bit in response to every Forward Traffic Channel slot that is associated with a detected preamble directed to the access terminal. Otherwise, the ACK Channel shall be gated off. When the ACK Channel bit is transmitted, it shall be transmitted on the first half slot on Walsh channel W_4^8.

For the Reverse Traffic Channel, the encoded RRI symbols shall be time-division multiplexed with the Pilot Channel, and the encoded RRI symbols shall be allocated the first 256 chips of every slot as shown in Figure 9.2.1.3.1-4.

Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6 give examples of the ACK Channel operation for a 153.6-kbps Forward Traffic Channel. The 153.6-kbps Forward Traffic Channel physical layer packets use four slots, and these slots are transmitted with a three-slot interval between them, as shown in the figures. The slots from other physical layer packets are interlaced in the three intervening slots.

Figure 9.2.1.3.1-5 shows the case of a normal physical layer packet termination. In this case, the access terminal transmits NAK responses on the ACK Channel after the first three slots of the physical layer packet are received indicating that it was unable to correctly receive the Forward Traffic Channel physical layer packet after only one, two, or three of the nominal four slots. An ACK or NAK is also transmitted after the last slot is received, as shown.

Figure 9.2.1.3.1-6 shows the case where the Forward Traffic Channel physical layer packet transmission is terminated early. In this example, the access terminal transmits an ACK response on the ACK Channel after the third slot is received indicating that it has correctly received the physical layer packet. When the access network receives such an ACK response, it does not transmit the remaining slots of the physical layer packet. Instead, it may begin transmission of any subsequent physical layer packets.

When the access terminal has received all slots of a physical layer packet or has transmitted a positive ACK response, the physical layer shall return *ForwardTrafficCompleted* indication.

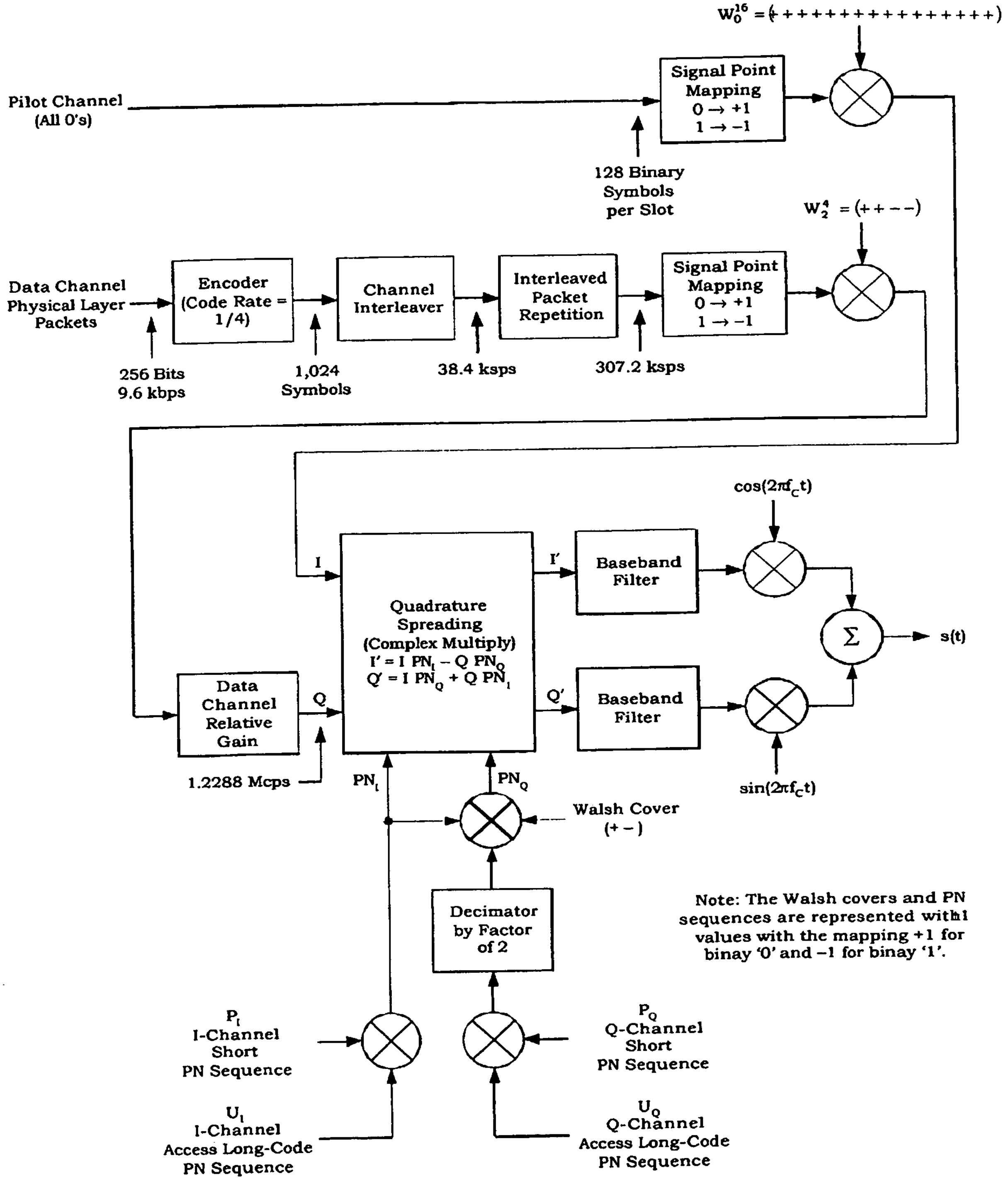
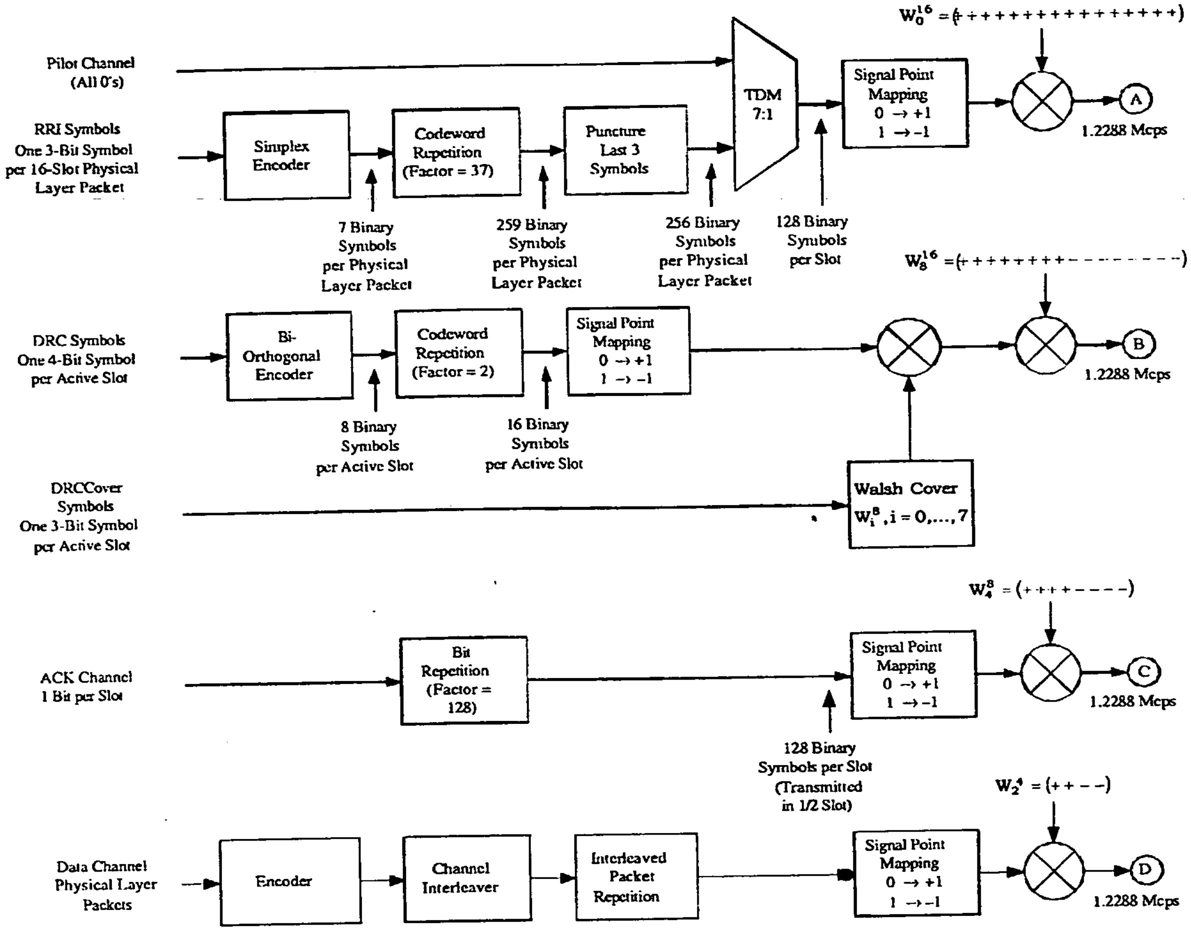

W_0^{16} = (+ + + + + + + + + + + + + + + +)
Pilot Channel (All 0's)
Signal Point Mapping 0 → +1 1 → −1
128 Binary Symbols per Slot
W_2^4 = (+ + − −)
Data Channel Physical Layer Packets
Encoder (Code Rate = 1/4)
Channel Interleaver
Interleaved Packet Repetition
Signal Point Mapping 0 → +1 1 → −1
256 Bits 9.6 kbps
1,024 Symbols
38.4 ksps
307.2 ksps
cos(2πf_C t)
I
I′
Baseband Filter
Quadrature Spreading (Complex Multiply)
I′ = I PN_I − Q PN_Q
Q′ = I PN_Q + Q PN_I
Σ
s(t)
Data Channel Relative Gain
Q
Q′
Baseband Filter
1.2288 Mcps
PN_I
PN_Q
sin(2πf_C t)
Walsh Cover (+ −)
Decimator by Factor of 2
Note: The Walsh covers and PN sequences are represented with±1 values with the mapping +1 for binay '0' and −1 for binay '1'.
P_I I-Channel Short PN Sequence
P_Q Q-Channel Short PN Sequence
U_I I-Channel Access Long-Code PN Sequence
U_Q Q-Channel Access Long-Code PN Sequence

Figure 9.2.1.3.1-1. Reverse Channel Structure for the Access Channel


W_0^{16} = (+ + + + + + + + + + + + + + + +)
Pilot Channel (All 0's)
RRI Symbols One 3-Bit Symbol per 16-Slot Physical Layer Packet
Simplex Encoder
Codeword Repetition (Factor = 37)
Puncture Last 3 Symbols
TDM 7:1
Signal Point Mapping 0 → +1 1 → -1
A
1.2288 Mcps
7 Binary Symbols per Physical Layer Packet
259 Binary Symbols per Physical Layer Packet
256 Binary Symbols per Physical Layer Packet
128 Binary Symbols per Slot
W_8^{16} = (+ + + + + + + + − − − − − − − −)
DRC Symbols One 4-Bit Symbol per Active Slot
Bi-Orthogonal Encoder
Codeword Repetition (Factor = 2)
Signal Point Mapping 0 → +1 1 → -1
B
1.2288 Mcps
8 Binary Symbols per Active Slot
16 Binary Symbols per Active Slot
DRCCover Symbols One 3-Bit Symbol per Active Slot
Walsh Cover W_i^8, i = 0,...,7
W_4^8 = (+ + + + − − − −)
ACK Channel 1 Bit per Slot
Bit Repetition (Factor = 128)
Signal Point Mapping 0 → +1 1 → -1
C
1.2288 Mcps
128 Binary Symbols per Slot (Transmitted in 1/2 Slot)
W_2^4 = (+ + − −)
Data Channel Physical Layer Packets
Encoder
Channel Interleaver
Interleaved Packet Repetition
Signal Point Mapping 0 → +1 1 → -1
D
1.2288 Mcps

Physical Layer Packets		Code			
Bits	Rate (kbps)	Rate	Symbols	Rate (ksps)	Rate (ksps)
256	9.6	1/4	1,024	38.4	307.2
512	19.2	1/4	2,048	76.8	307.2
1,024	38.4	1/4	4,096	153.6	307.2
2,048	76.8	1/4	8,192	307.2	307.2
4,096	153.6	1/2	8,192	307.2	307.2

Note: The Walsh covers are represented with ±1 values with the mapping +1 for '0' and −1 for '1'.

Figure 9.2.1.3.1-2. Reverse Channel Structure for the Reverse Traffic Channel (Part 1 of 2)

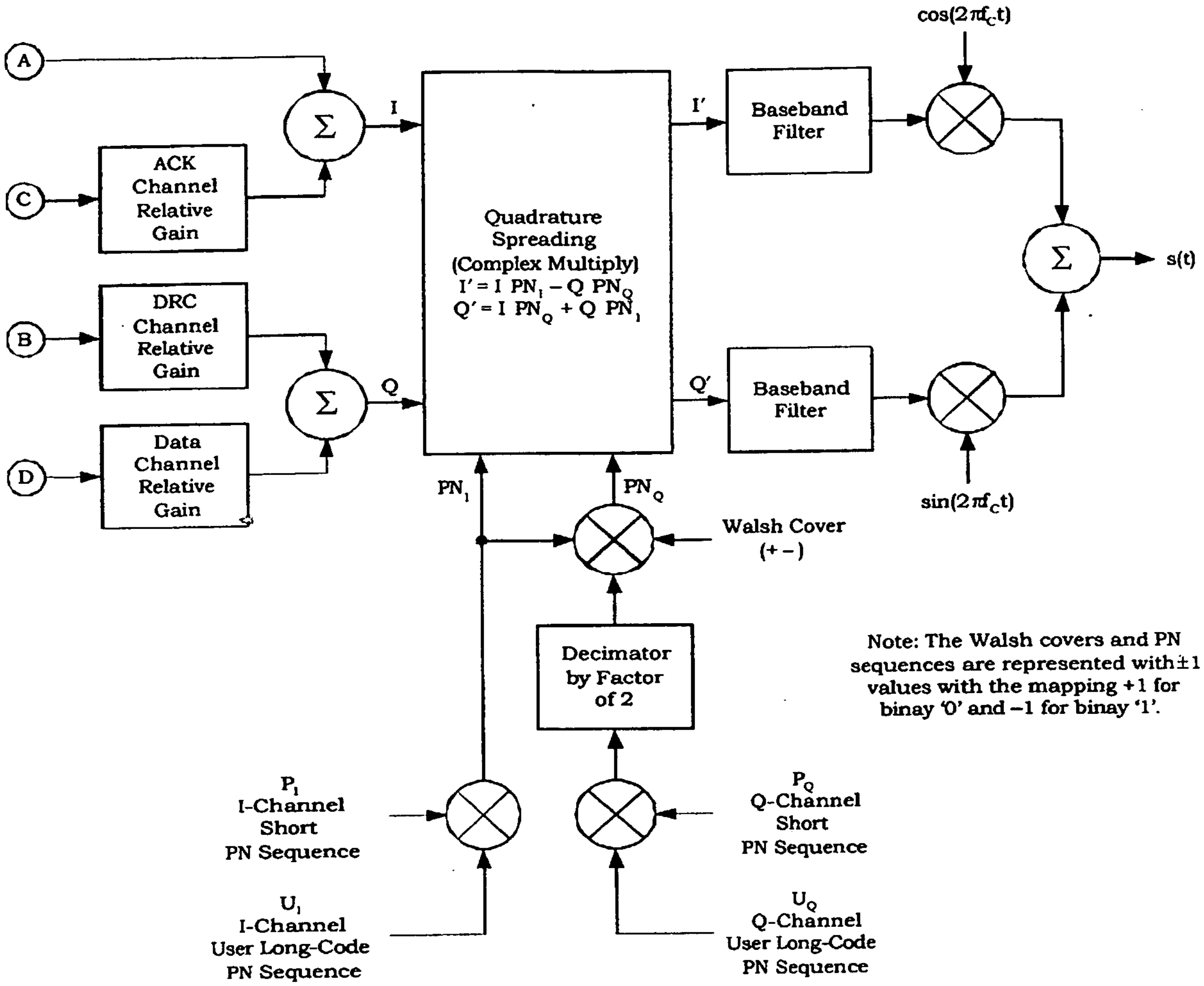

cos(2πf_Ct)
A
C
B
D
ACK Channel Relative Gain
DRC Channel Relative Gain
Data Channel Relative Gain
Σ
I
Q
Quadrature Spreading (Complex Multiply)
I′ = I PN_I − Q PN_Q
Q′ = I PN_Q + Q PN_I
I′
Q′
Baseband Filter
Baseband Filter
Σ
s(t)
sin(2πf_Ct)
PN_I
PN_Q
Walsh Cover (+ −)
Decimator by Factor of 2
Note: The Walsh covers and PN sequences are represented with ±1 values with the mapping +1 for binay '0' and −1 for binay '1'.
P_I I-Channel Short PN Sequence
P_Q Q-Channel Short PN Sequence
U_I I-Channel User Long-Code PN Sequence
U_Q Q-Channel User Long-Code PN Sequence

Figure 9.2.1.3.1-3. Reverse Channel Structure for the Reverse Traffic Channel (Part 2 of 2)

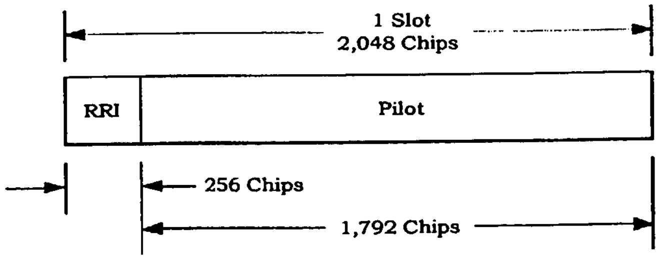


Figure 9.2.1.3.1-4. Pilot Channel and RRI Channel TDM Allocations for the Reverse Traffic Channel

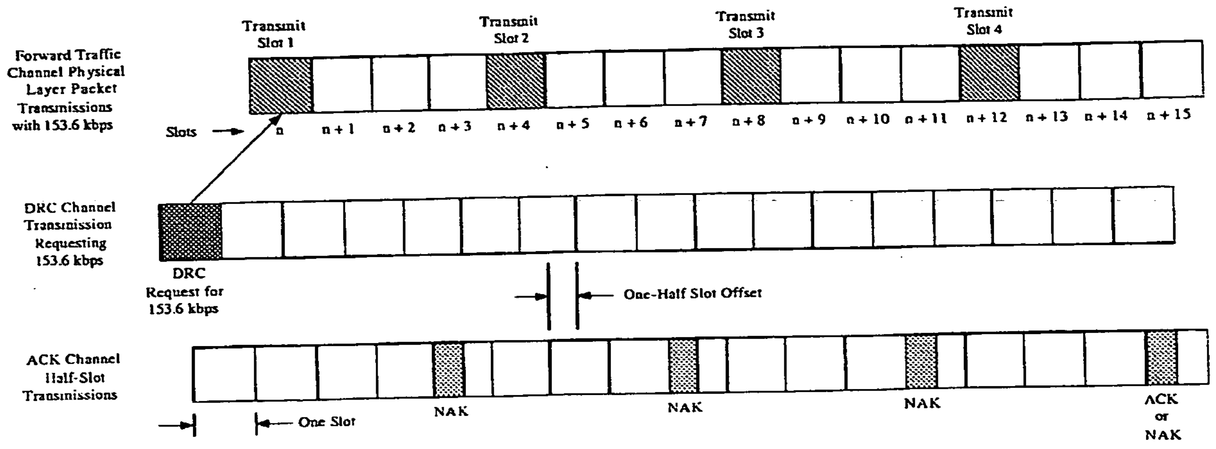


Figure 9.2.1.3.1-5. Multislot Physical Layer Packet with Normal Termination

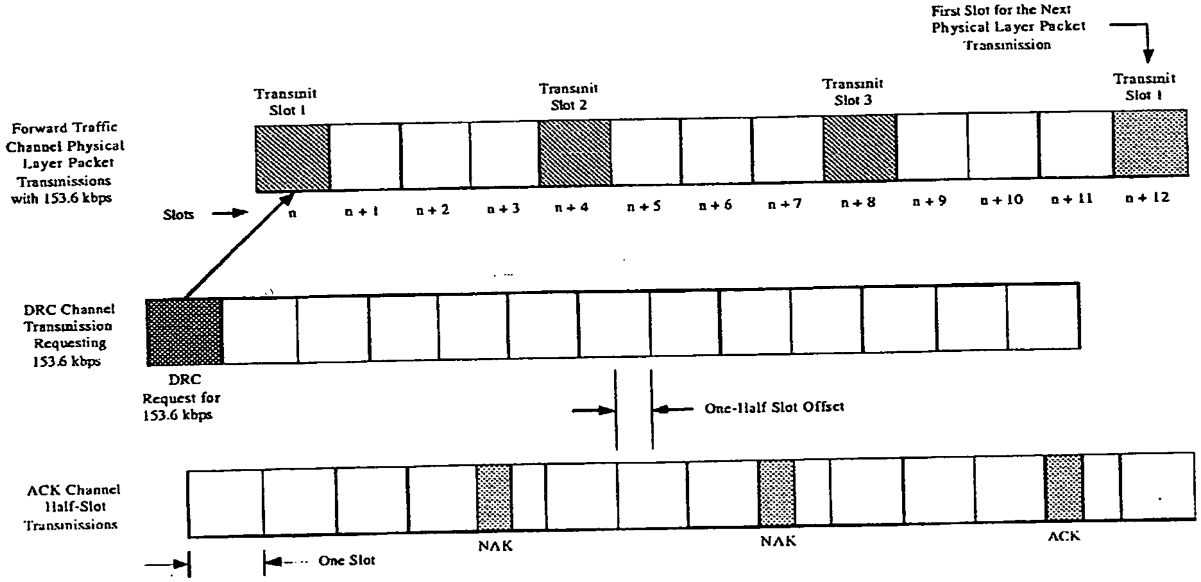

First Slot for the Next Physical Layer Packet Transmission
Forward Traffic Channel Physical Layer Packet Transmissions with 153.6 kbps
Transmit Slot 1
Transmit Slot 2
Transmit Slot 3
Transmit Slot 1
Slots
n
n + 1
n + 2
n + 3
n + 4
n + 5
n + 6
n + 7
n + 8
n + 9
n + 10
n + 11
n + 12
DRC Channel Transmission Requesting 153.6 kbps
DRC Request for 153.6 kbps
One-Half Slot Offset
ACK Channel Half-Slot Transmissions
One Slot
NAK
NAK
ACK

Figure 9.2.1.3.1-6. Multislot Physical Layer Packet with Early Termination

9.2.1.3.1.1 Modulation Parameters

The modulation parameters for the Access Channel and the Reverse Traffic Channel shall be as specified in Table 9.2.1.3.1.1-1.

Table 9.2.1.3.1.1-1. Modulation Parameters for the Access Channel and the Reverse Traffic Channel

	Data Rate (kbps)				
Parameter	9.6	19.2	38.4	76.8	153.6
Reverse Rate Index	1	2	3	4	5
Bits per Physical Layer Packet	256	512	1,024	2,048	4,096
Physical Layer Packet Duration (ms)	26.66...	26.66...	26.66...	26.66...	26.66...
Code Rate	1/4	1/4	1/4	1/4	1/2
Code Symbols per Physical Layer Packet	1,024	2,048	4,096	8,192	8,192
Code Symbol Rate (ksps)	38.4	76.8	153.6	307.2	307.2
Interleaved Packet Repeats	8	4	2	1	1
Modulation Symbol Rate (ksps)	307.2	307.2	307.2	307.2	307.2
Modulation Type	BPSK	BPSK	BPSK	BPSK	BPSK
PN Chips per Physical Layer Packet Bit	128	64	32	16	8

9.2.1.3.1.2 Data Rates

The access terminal shall transmit information on the Access Channel at a fixed data rate of 9.6 kbps.

The access terminal shall transmit information on the Reverse Traffic Channel at a variable data rate of 9.6, 19.2, 38.4, 76.8, or 153.6 kbps, according to the Reverse Traffic Channel MAC Protocol.

9.2.1.3.2 Access Channel

The Access Channel is used by the access terminal to initiate communication with the access network or to respond to an access terminal directed message. The Access Channel consists of a Pilot Channel and a Data Channel as shown in Figure 9.2.1.3.1-1.

An access probe shall consist of a preamble followed by one or more Access Channel physical layer packets. During the preamble transmission, only the Pilot Channel is transmitted. During the Access Channel physical layer packet transmission, both the Pilot Channel and the Data Channel are transmitted. The output power of the Pilot Channel during the preamble portion of an access probe is higher than it is during the data portion of the probe by an amount such that the total output power of the preamble and data portions of the access probe are the same as shown in Figure 9.2.1.3.2-1.

The preamble length is specified by the parameter PreambleLength which is public data from the Access Channel MAC Protocol. The Access Channel physical layer packets are transmitted at a fixed data rate of 9.6 kbps.

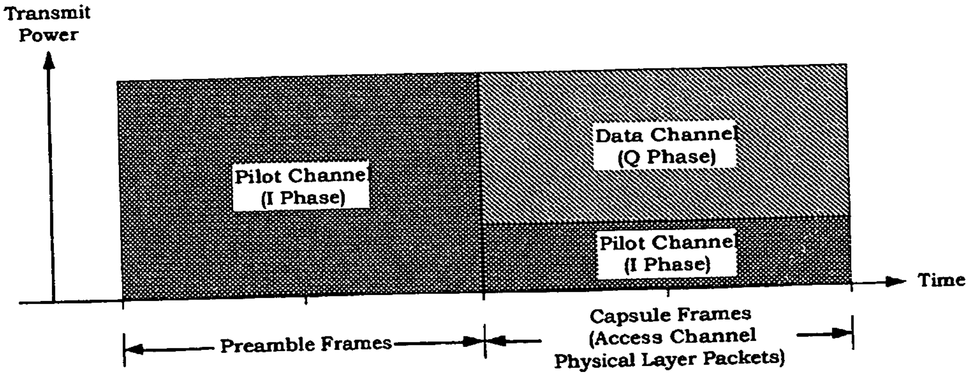


Figure 9.2.1.3.2-1. Example of an Access Probe

9.2.1.3.2.1 Pilot Channel

The access terminal shall transmit unmodulated symbols with a binary value of '0' on the Pilot Channel. The Pilot Channel shall be transmitted continuously during Access Channel transmission. It shall be transmitted on the I channel using the 16-chip Walsh function number 0 (W_0^{16} = + + + + + + + + + + + + + + + +) cover.

9.2.1.3.2.2 Data Channel

One or more Access Channel physical layer packets shall be transmitted on the Data Channel during every access probe. The Access Channel physical layer packets shall be transmitted at a fixed data rate of 9.6 kbps on the Q channel using the 4-chip Walsh function number 2 (W_2^4 = + + – –). The Access Channel physical layer packets shall be preceded by a preamble of PreambleLength frames where only the Pilot Channel is transmitted. The PreambleLength parameter is public data from the Access Channel MAC Protocol.

9.2.1.3.3 Reverse Traffic Channel

The Reverse Traffic Channel is used by the access terminal to transmit user-specific traffic or signaling information to the access network. The Reverse Traffic Channel consists of a Pilot Channel, an RRI Channel, a DRC Channel, an ACK Channel, and a Data Channel.

The access terminal shall support transmission of information on the Data Channel of the Reverse Traffic Channel at data rates of 9.6, 19.2, 38.4, 76.8, and 153.6 kbps. The data rate used on the Data Channel is specified by the Reverse Traffic Channel MAC Protocol. The gain of the Data Channel relative to that of the Pilot Channel for the Reverse Traffic Channel depends on the data rate as shown in Table 9.2.1.2.4.1-1.

9.2.1.3.3.1 Pilot Channel

The access terminal shall transmit unmodulated symbols with a binary value of '0' on the Pilot Channel. The transmission of the Pilot Channel and the RRI Channel shall be time multiplexed on the same Walsh channel as shown in Figure 9.2.1.3.1-2. The Pilot Channel and the RRI Channel shall be transmitted at the same power.

9.2.1.3.3.2 Reverse Rate Indicator Channel

The RRI Channel is used by the access terminal to indicate the data rate at which the Data Channel is transmitted. The data rate is represented by a three-bit RRI symbol at the rate of one 3-bit symbol per 16-slot physical layer packet. Each RRI symbol shall be encoded into a 7-bit codeword by a simplex encoder as specified in Table 9.2.1.3.3.2-1. Then, each codeword shall be repeated 37 times and the last 3 symbols shall be disregarded (i.e., punctured), as shown in Figure 9.2.1.3.1-2. The resulting 256 binary symbols per physical layer packet shall be time-division multiplexed with the Pilot Channel symbols and span the same time interval as the corresponding physical layer packet. The time-division-multiplexed Pilot and RRI Channel sequence shall be spread with the 16-chip Walsh function W_0^{16} producing 256 RRI chips per slot. The RRI chips shall be time-division multiplexed into the first 256 chips of every slot as shown in Figure 9.2.1.3.1-4. When no physical layer packet is transmitted on the Reverse Traffic Channel, the access terminal shall transmit the zero data rate RRI codeword on the RRI Channel, as specified in Table 9.2.1.3.3.2-1I The Pilot Channel and the RRI Channel shall be transmitted on the channel.

Table 9.2.1.3.3.2-1. RRI Symbol and Simplex Encoder Assignments

Data Rate (kbps)	RRI Symbol	RRI Codeword
0	000	0000000
9.6	001	1010101
19.2	010	0110011
38.4	011	1100110
76.8	100	0001111
153.6	101	1011010
Reserved	110	0111100
Reserved	111	1101001

9.2.1.3.3.3 Data Rate Control Channel

The DRC Channel is used by the access terminal to indicate to the access network the selected serving sector and the requested data rate on the Forward Traffic Channel. The requested Forward Traffic Channel data rate is mapped into a four-bit DRC value as specified by the Forward Traffic Channel MAC Protocol. An 8-ary Walsh function corresponding to the selected serving sector is used to spread the DRC Channel transmission. The cover mapping is defined by the public data DRCCover from the Forward Traffic Channel MAC Protocol.

The DRC values shall be transmitted at a data rate of 600/DRCLength DRC values per second, where DRCLength is public data from the Forward Traffic Channel MAC Protocol. When DRCLength is greater than one, the DRC value and DRCCover inputs in Figure 9.2.1.3.1-2 are repeated for DRCLength consecutive slots as specified in the Forward Traffic Channel MAC Protocol.

The DRC values shall be block encoded to yield 8-bit bi-orthogonal codewords, as specified in Table 9.2.1.3.3.3-1. Each DRC codeword shall be transmitted twice per slot. Each bit of a repeated codeword shall be spread by an 8-ary Walsh function W_i^8 as defined in Table 9.2.1.3.3.3-2, where i equals DRCCover. Each Walsh chip of the 8-ary Walsh function shall be further spread by the Walsh function W_8^{16}. Each DRC value shall be transmitted over DRCLength slots when the DRC Channel is continuously transmitted.

The access terminal may support gated DRC transmissions. For an access terminal that supports gated DRC transmissions, it shall gate its DRC transmissions if DRCGating equals 1, where DRCGating is public data from the Forward Traffic Channel MAC Protocol. When the DRC transmissions are gated, each DRC symbol shall be transmitted over only one of every DRCLength slots as specified in the Forward Traffic Channel MAC Protocol. Slots where the DRC Channel is not gated off are called active slots.

The DRC Channel shall be transmitted on the Q Channel as shown in Figure 9.2.1.3.1-3.

The timing of the Forward Traffic Channel transmission corresponding to a DRC symbol shall be as specified by the Forward Traffic Channel MAC Protocol. The transmission of DRC symbols shall start at the mid-slot point. The timing for the Default Forward Traffic Channel MAC Protocol is shown in Figure 9.2.1.3.3.3-1 and Figure 9.2.1.3.3.3-2.

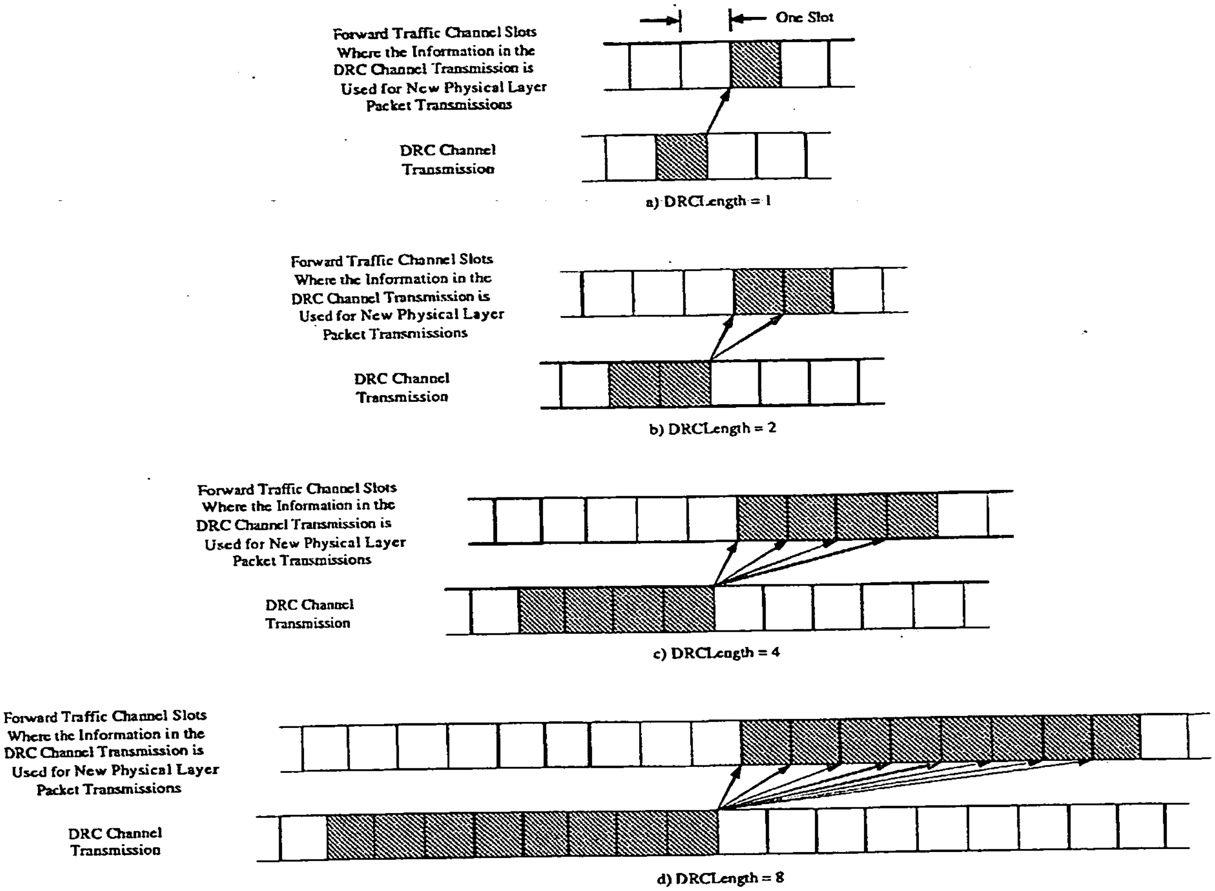
Table 9.2.1.3.3.3-1. DRC Bi-Orthogonal Encoding[43]

DRC Value	Codeword
0x0	00000000
0x1	11111111
0x2	01010101
0x3	10101010
0x4	00110011
0x5	11001100
0x6	01100110
0x7	10011001
0x8	00001111
0x9	11110000
0xA	01011010
0xB	10100101
0xC	00111100
0xD	11000011
0xE	01101001
0xF	10010110

Table 9.2.1.3.3.3-2. 8-ary Walsh Functions

W_0^8	0000 0000
W_1^8	0101 0101
W_2^8	0011 0011
W_3^8	0110 0110
W_4^8	0000 1111
W_5^8	0101 1010
W_6^8	0011 1100
W_7^8	0110 1001

[43] The correspondence between data rates and DRC values is defined in Forward Traffic Channel MAC protocol (see Table 8.4.5.5.1.1-1).


One Slot
Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission

a) DRCLength = 1

Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission

b) DRCLength = 2

Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission

c) DRCLength = 4

Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission

d) DRCLength = 8

Figure 9.2.1.3.3.3-1. DRC Timing for Nongated Transmission

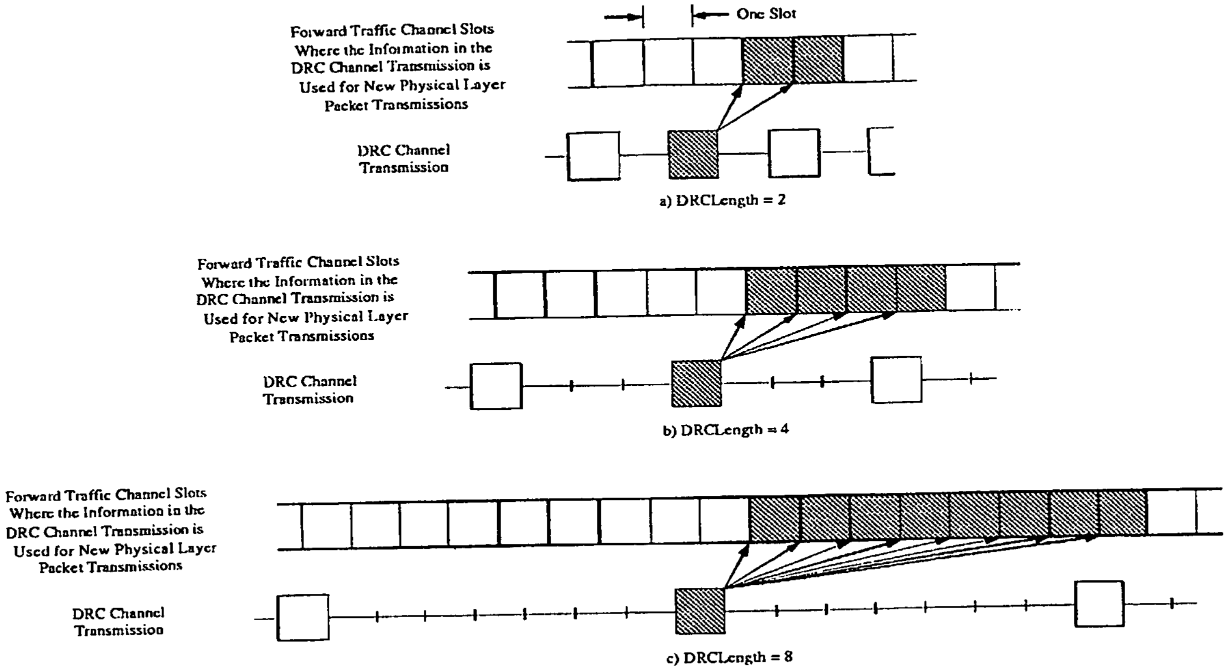

One Slot
Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission
a) DRCLength = 2
Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission
b) DRCLength = 4
Forward Traffic Channel Slots Where the Information in the DRC Channel Transmission is Used for New Physical Layer Packet Transmissions
DRC Channel Transmission
c) DRCLength = 8

Figure 9.2.1.3.3.3-2. DRC Timing for Gated Transmission

9.2.1.3.3.4 ACK Channel

The ACK Channel is used by the access terminal to inform the access network whether a physical layer packet transmitted on the Forward Traffic Channel has been received successfully or not. The access terminal shall transmit an ACK Channel bit in response to every Forward Traffic Channel slot that is associated with a detected preamble directed to the access terminal. The access terminal shall transmit at most one redundant positive ACK in response to a Forward Traffic Channel slot that is detected as a continuation of the physical layer packet that has been successfully received. Otherwise, the ACK Channel shall be gated off.

The ACK Channel shall be BPSK modulated. A '0' bit (ACK) shall be transmitted on the ACK Channel if a Forward Traffic Channel physical layer packet has been successfully received; otherwise, a '1' bit (NAK) shall be transmitted. A Forward Traffic Channel physical layer packet is considered successfully received if the FCS checks. For a Forward Traffic Channel physical layer packet transmitted in slot n on the Forward Channel, the corresponding ACK Channel bit shall be transmitted in slot n + 3 on the Reverse Channel (see Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6). The ACK Channel transmission shall be transmitted in the first half of the slot and shall last for 1024 PN chips as shown in Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6. The ACK Channel shall use the Walsh channel identified by the Walsh function W_4^8 and shall be transmitted on the I channel.

9.2.1.3.3.5 Data Channel

The Data Channel shall be transmitted at the data rates given in Table 9.2.1.3.1.1-1. Data transmissions shall only begin at slot FrameOffset within a frame. The FrameOffset parameter is public data of the Reverse Traffic Channel MAC Protocol. All data transmitted on the Reverse Traffic Channel shall be encoded, block interleaved, sequence repeated, and orthogonally spread by Walsh function W_2^4.

9.2.1.3.4 Encoding

9.2.1.3.4.1 Reverse Link Encoder Structure and Parameters

The Reverse Traffic Channel and Access Channel physical layer packets shall be encoded with code rates of 1/2 or 1/4, depending on the data rate. First, the encoder shall discard the six bits of the TAIL field in the physical layer packet inputs (i.e., it shall discard the last six bits in the input physical layer packets). Then, it shall encode the remaining bits with a turbo encoder, as specified in 9.2.1.3.4.2. The turbo encoder will add an internally generated tail.

The encoder parameters shall be as specified in Table 9.2.1.3.4.1-1.

Table 9.2.1.3.4.1-1. Parameters for the Reverse Link Encoder

Data Rate (kbps)	9.6	19.2	38.4	76.8	153.6
Reverse Rate Index	1	2	3	4	5
Code Rate	1/4	1/4	1/4	1/4	1/2
Bits per Physical Layer Packet	256	512	1,024	2,048	4,096
Number of Turbo Encoder Input Symbols	250	506	1,018	2,042	4,090
Turbo Encoder Code Rate	1/4	1/4	1/4	1/4	1/2
Encoder Output Block Length (Code Symbols)	1,024	2,048	4,096	8,192	8,192

9.2.1.3.4.2 Turbo Encoding

The turbo encoder encodes the input data and adds an output tail sequence. If the total number of input bits is N_{turbo}, the turbo encoder generates N_{turbo}/R encoded data output symbols followed by 6/R tail output symbols, where R is the code rate of 1/2 or 1/4. The turbo encoder employs two systematic, recursive, convolutional encoders connected in parallel, with an interleaver, the turbo interleaver, preceding the second recursive convolutional encoder.

The two recursive convolutional codes are called the constituent codes of the turbo code. The outputs of the constituent encoders are punctured and repeated to achieve the $(N_{turbo} + 6)/R$ output symbols.

9.2.1.3.4.2.1 Turbo Encoders

A common constituent code shall be used for the turbo codes of rate 1/2 and 1/4. The transfer function for the constituent code shall be

$$G(D) = \left[\frac{n_0(D)}{d(D)} \quad \frac{n_1(D)}{} \right]$$

where $d(D) = 1 + D^2 + D^3$, $n_0(D) = 1 + D + D^3$, and $n_1(D) = 1 + D + D^2 + D^3$.

The turbo encoder shall generate an output symbol sequence that is identical to the one generated by the encoder shown in Figure 9.2.1.3.4.2.2-1. Initially, the states of the constituent encoder registers in this figure are set to zero. Then, the constituent encoders are clocked with the switches in the positions noted.

The encoded data output symbols are generated by clocking the constituent encoders N_{turbo} times with the switches in the up positions and puncturing the outputs as specified in Table 9.2.1.3.4.2.2-1. Within a puncturing pattern, a '0' means that the symbol shall be deleted and a '1' means that a symbol shall be passed. The constituent encoder outputs for each bit period shall be output in the sequence X, Y_0, Y_1, X', Y'_0, Y'_1 with the X output first. Symbol repetition is not used in generating the encoded data output symbols.

9.2.1.3.4.2.2 Turbo Code Termination

The turbo encoder shall generate 6/R tail output symbols following the encoded data output symbols. This tail output symbol sequence shall be identical to the one generated by the encoder shown in Figure 9.2.1.3.4.2.2-1. The tail output symbols are generated after the constituent encoders have been clocked N_{turbo} times with the switches in the up position. The first 3/R tail output symbols are generated by clocking Constituent Encoder 1 three times with its switch in the down position while Constituent Encoder 2 is not clocked and puncturing and repeating the resulting constituent encoder output symbols. The last 3/R tail output symbols are generated by clocking Constituent Encoder 2 three times with its switch in the down position while Constituent Encoder 1 is not clocked and puncturing and repeating the resulting constituent encoder output symbols. The constituent encoder outputs for each bit period shall be output in the sequence X, Y_0, Y_1, X', Y'_0, Y'_1 with the X output first.

The constituent encoder output symbol puncturing and symbol repetition shall be as specified in Table 9.2.1.3.4.2.2-2. Within a puncturing pattern, a '0' means that the symbol shall be deleted and a '1' means that a symbol shall be passed. For rate-1/2 turbo codes, the tail output symbols for each of the first three tail bit periods shall be XY_0, and the tail output symbols for each of the last three tail bit periods shall be $X'Y'_0$. For rate-1/4 turbo codes, the tail output symbols for each of the first three tail bit periods shall be XXY_0Y_1, and the tail output symbols for each of the last three tail bit periods shall be $X'X'Y'_0Y'_1$.

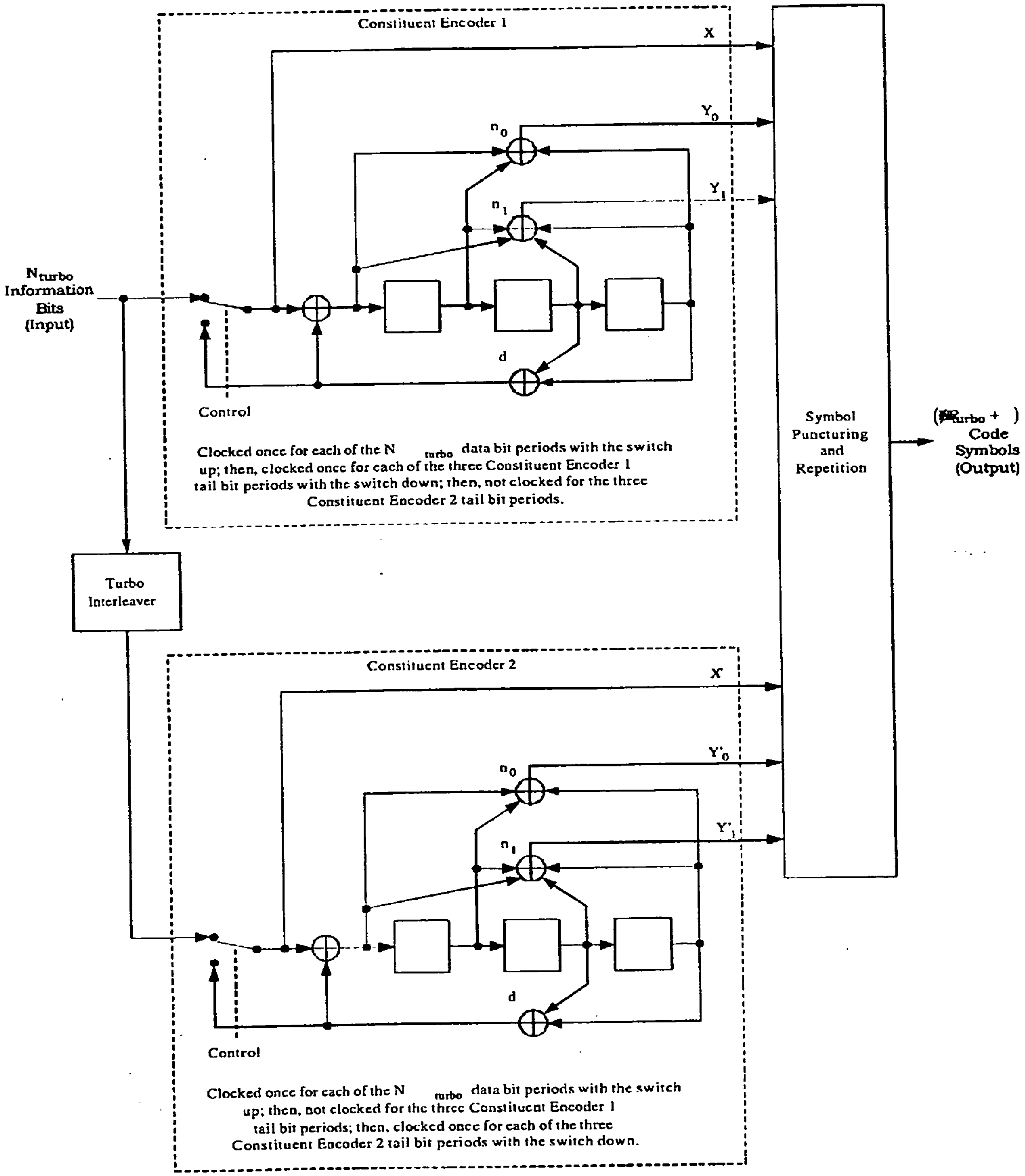

Constituent Encoder 1
X
Y0
n0
Y1
n1
Nturbo Information Bits (Input)
d
Control
Clocked once for each of the N turbo data bit periods with the switch up; then, clocked once for each of the three Constituent Encoder 1 tail bit periods with the switch down; then, not clocked for the three Constituent Encoder 2 tail bit periods.
Turbo Interleaver
Symbol Puncturing and Repetition
(Nturbo +) Code Symbols (Output)
Constituent Encoder 2
X'
Y'0
n0
Y'1
n1
d
Control
Clocked once for each of the N turbo data bit periods with the switch up; then, not clocked for the three Constituent Encoder 1 tail bit periods; then, clocked once for each of the three Constituent Encoder 2 tail bit periods with the switch down.

Figure 9.2.1.3.4.2.2-1. Turbo Encoder

Table 9.2.1.3.4.2.2-1. Puncturing Patterns for the Data Bit Periods

	Code Rate	
Output	1/2	1/4
X	11	11
Y_0	10	11
Y_1	00	10
X′	00	00
Y'_0	01	01
Y'_1	00	11

Note: For each rate, the puncturing table shall be read first from top to bottom and then from left to right.

Table 9.2.1.3.4.2.2-2. Puncturing Patterns for the Tail Bit Periods

	Code Rate	
Output	1/2	1/4
X	111 000	111 000
Y_0	111 000	111 000
Y_1	000 000	111 000
X′	000 111	000 111
Y'_0	000 111	000 111
Y'_1	000 000	000 111

Note: For rate-1/2 turbo codes, the puncturing table shall be read first from top to bottom and then from left to right. For rate-1/4 turbo codes, the puncturing table shall be read first from top to bottom repeating X and X′, and then from left to right.

9.2.1.3.4.2.3 Turbo Interleavers

The turbo interleaver, which is part of the turbo encoder, shall block interleave the turbo encoder input data that is fed to Constituent Encoder 2.

The turbo interleaver shall be functionally equivalent to an approach where the entire aequence of turbo interleaver input bits are written sequentially into an array at sequence of addresses, and then the entire sequence is read out from a sequence of addresses that are defined by the procedure described below.

Let the sequence of input addresses be from 0 to N_{turbo} – 1. Then, the sequence of interleaver output addresses shall be equivalent to those generated by the procedure illustrated in Figure 9.2.1.3.4.2.3-1 and described below.[44]

1. Determine the turbo interleaver parameter, n, where n is the smallest integer such that $N_{turbo} \leq 2^{n+5}$. Table 9.2.1.3.4.2.3-1 gives this parameter for the different physical layer packet sizes.
2. Initialize an (n + 5)-bit counter to 0.
3. Extract the n most significant bits (MSBs) from the counter and add one to form a new value. Then, discard all except the n least significant bits (LSBs) of this value.
4. Obtain the n-bit output of the table lookup defined in Table 9.2.1.3.4.2.3-2 with a read address equal to the five LSBs of the counter. Note that this table depends on the value of n.
5. Multiply the values obtained in Steps 3 and 4, and discard all except the n LSBs.
6. Bit-reverse the five LSBs of the counter.
7. Form a tentative output address that has its MSBs equal to the value obtained in Step 6 and its LSBs equal to the value obtained in Step 5.
8. Accept the tentative output address as an output address if it is less than N_{turbo}; otherwise, discard it.
9. Increment the counter and repeat Steps 3 through 8 until all N_{turbo} interleaver output addresses are obtained.

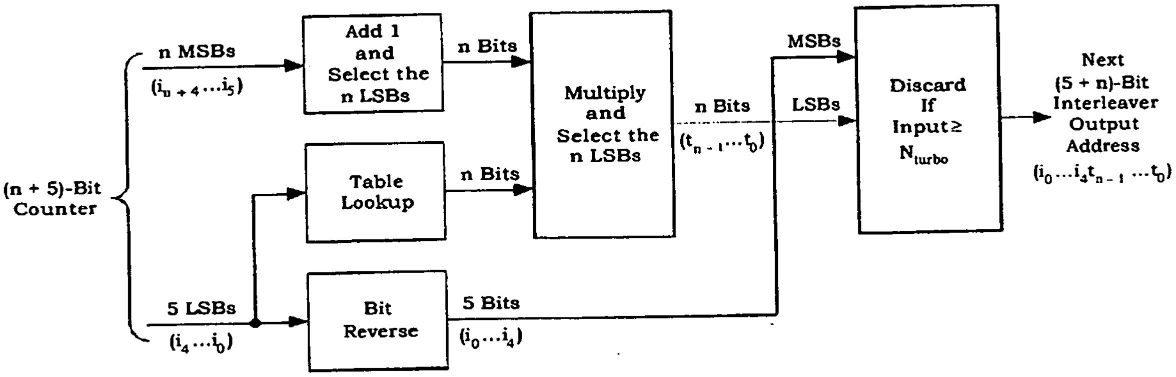

(n + 5)-Bit Counter
n MSBs
$(i_{n+4} \dots i_5)$
5 LSBs
$(i_4 \dots i_0)$
Add 1 and Select the n LSBs
Table Lookup
Bit Reverse
n Bits
n Bits
5 Bits
$(i_0 \dots i_4)$
Multiply and Select the n LSBs
n Bits
$(t_{n-1} \dots t_0)$
MSBs
LSBs
Discard If Input≥ N_{turbo}
Next (5 + n)-Bit Interleaver Output Address
$(i_0 \dots i_4 t_{n-1} \dots t_0)$

Figure 9.2.1.3.4.2.3-1. Turbo Interleaver Output Address Calculation Procedure

[44] This procedure is equivalent to one where the counter values are written into a 2^5-row by 2^n-column array by rows, the rows are shuffled according to a bit-reversal rule, the elements within each row are permuted according to a row-specific linear congruential sequence, and tentativ output addresses are read out by column. The linear congruential sequence rule is x(i + 1) = (x(i) + c) mod 2^n, where x(0) = c and c is a row-specific value from a table lookup.

Table 9.2.1.3.4.2.3-1. Turbo Interleaver Parameter

Physical Layer Packet Size	Turbo Interleaver Block Size N_{turbo}	Turbo Interleaver Parameter n
256	250	3
512	506	4
1,024	1,018	5
2,048	2,042	6
4,096	4,090	7

Table 9.2.1.3.4.2.3-2. Turbo Interleaver Lookup Table Definition

Table Index	n = 3 Entries	n = 4 Entries	n = 5 Entries	n = 6 Entries	n = 7 Entries
0	1	5	27	3	15
1	1	15	3	27	127
2	3	5	1	15	89
3	5	15	15	13	1
4	1	1	13	29	31
5	5	9	17	5	15
6	1	9	23	1	61
7	5	15	13	31	47
8	3	13	9	3	127
9	5	15	3	9	17
10	3	7	15	15	119
11	5	11	3	31	15
12	3	15	13	17	57
13	5	3	1	5	123
14	5	15	13	39	95
15	1	5	29	1	5
16	3	13	21	19	85
17	5	15	19	27	17
18	3	9	1	15	55
19	5	3	3	13	57
20	3	1	29	45	15
21	5	3	17	5	41
22	5	15	25	33	93
23	5	1	29	15	87
24	1	13	9	13	63
25	5	1	13	9	15
26	1	9	23	15	13
27	5	15	13	31	15
28	3	11	13	17	81
29	5	3	1	5	57
30	5	15	13	15	31
31	3	5	13	33	69

9.2.1.3.5 Channel Interleaving

The sequence of binary symbols at the output of the encoder shall be interleaved with a bit-reversal channel interleaver.

The bit-reversal channel interleaver shall be functionally equivalent to an approach where the entire sequence of symbols to be interleaved is written into a linear sequential array with addresses from 0 to $2^L - 1$ and they are read out from a sequence of addresses based on the procedure described below.

2.? The sequence of array addresses from which the interleaved symbols are read out is generated by a bit-reversal address generator.

?.? The ith interleaved symbol is read out from the array element at address A_i that satisfies:

$$A_i = \text{Bit\_Reversal}(i, L)$$

where i = 0 to $2^L - 1$ and Bit_Reversal(y, L) indicates the bit-reversed L-bit value of y such that if i is expressed in the binary form of $i = b_{L-1}b_{L-2}\ldots b_1b_0$, where b_k = 0 or 1, b_0 is the LSB and b_L is the MSB, $A_i = b_0b_1\ldots b_{L-2}b_{L-1}$.

2.? The bit-reversal interleaving process is completed when all of the symbols in the entire linear array are read out.

Figure 9.2.1.3.5-1 illustrates the procedure for generating the channel interleaver output address.

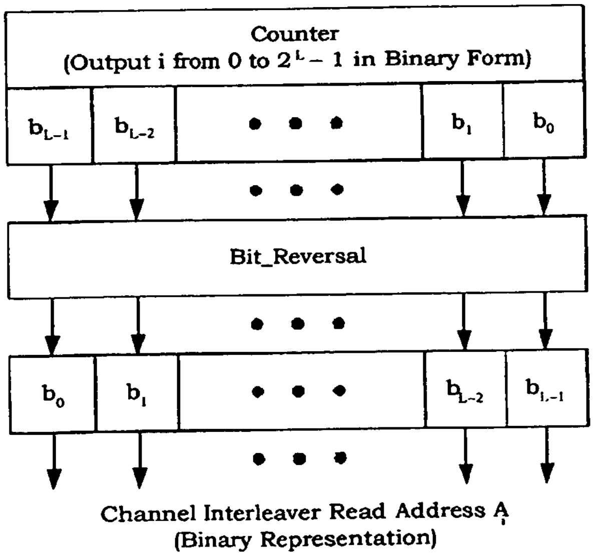


Figure 9.2.1.3.5-1. Channel Interleaver Address Generation

9.2.1.3.6 Sequence Repetition

If the data rate is lower than 76.8 kbps, the sequence of interleaved code symbols shall be repeated before being modulated. The number of repeats varies for each data rate and shall be as specified in Table 9.2.1.3.1.1-1. The repetition shall be functionally equivalent to sequentially reading out all the symbols from the interleaver memory as many times as necessary to achieve the fixed 307.2-ksps modulation symbol rate.

9.2.1.3.7 Orthogonal Covers

The Pilot Channel, consisting of the time-division-multiplexed Pilot and RRI Channels, the DRC Channel, the ACK Channel, and the Data Channel shall be spread with Walsh functions, also called Walsh covers, at a fixed chip rate of 1.2288 Mcps. Walsh function time alignment shall be such that the first Walsh chip begins at a slot boundary referenced to the access terminal transmission time.

The Walsh cover assignments are shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-2. The Pilot Channel shall be covered by the 16-chip Walsh function number 0 W_0^{16} = + + + + + + + + + + + + + + + +). The DRC Channel shall be covered by the 16-chip Walsh function number 8 (W_8^{16} = + + + + + + + + – – – – – – – –). The ACK Channel shall be covered by the 8-chip Walsh function number 4 (W_4^8 = + + + + – – – –). The Data Channel shall be covered by the 4-chip Walsh function number 2 (W_2^4 = + + – –).

9.2.1.3.8 Quadrature Spreading

Following the orthogonal spreading, the ACK, DRC, and Data Channel chip sequences shall be scaled by a factor that gives the gain of each of these channels relative to that of the Pilot Channel. The relative gain values for the ACK and DRC Channels are specified by the parameters AckChannelGain and DRCChannelGain which are public data of the Forward Traffic Channel MAC Protocol. For the Reverse Traffic Channel, the relative gain of the Data Channel is specified by parameters that are public data of the Reverse Traffic Channel MAC Protocol as described in 9.2.1.2.4.1. For the Access Channel, the relative gain of the Data Channel is specified by parameters that are public data of the Access Channel MAC Protocol as described in 9.2.1.2.4.1.

After the scaling, the Pilot and scaled ACK, DRC, and Data Channel sequences are combined to form resultant I-Channel and Q-Channel sequences, and these sequences are quadrature spread as shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3. The quadrature spreading shall occur at the chip rate of 1.2288 Mcps, and it shall be used for the Reverse Traffic Channel and the Access Channel. The Pilot and scaled ACK Channel sequences shall be added to form the resultant I-Channel sequence, and the scaled DRC and Data Channel sequences shall be added to form the resultant Q-Channel sequence. The quadrature spreading operation shall be equivalent to a complex multiply operation of the resultant I-Channel and resultant Q-Channel sequences by the PN_I and PN_Q PN sequences, as shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3.

The I and Q PN sequences, PN_I and PN_Q, shall be obtained from the long-code PN sequences, U_I and U_Q, and the access terminal common short PN sequences, P_I and P_Q. The binary long-code PN sequence and short PN sequence values of '0' and '1' shall be mapped into values of +1 and −1, respectively.

The bipolar PN_I sequence values shall be equivalent to those obtained by multiplying the bipolar P_I values by the bipolar U_I values.

The bipolar PN_Q sequence values shall be equivalent to those obtained with the following procedure:

1. Multiply the bipolar P_Q values by the bipolar U_Q values.
2. Decimate the sequence of values obtained in Step 1 by a factor of two. That is, the decimator provides an output that is constant for two consecutive chips by deleting every other input value and repeating the previous input value in place of the deleted value. The retained values shall align with the first chip of a slot.
3. Multiply pairs of decimator output symbols by the Walsh cover sequence (+ −). That is, pass the first value of every pair unchanged and multiply the second value of every pair by −1.
4. Multiply the sequence obtained in Step 3 by the bipolar PN_I sequence.

9.2.1.3.8.1 Access Terminal Common Short-Code PN Sequences

The access terminal common short-code PN sequences shall be the zero-offset I and Q PN sequences with a period of ^{15} chips, and they shall be based on the following characteristic polynomials, respectively:

$$P_I(x) = x^{15} + x^{13} + x^9 + x^8 + x^7 + x^5 + 1$$

(for the in-phase (I) sequence)

and

$$P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$$

(for the quadrature-phase (Q) sequence).

The maximum length linear feedback shift-register sequences {I(n)} and {Q(n)} based on the above are of length $2^{15} - 1$ and can be generated by the following linear recursions:

$$I(n) = I(n-15) \oplus I(n-10) \oplus I(n-8) \oplus I(n-7) \oplus I(n-6) \oplus I(n-2)$$

(based on $P_I(x)$ as the characteristic polynomial)

and

$$Q(n) = Q(n-15) \oplus Q(n-12) \oplus Q(n-11) \oplus Q(n-10) \oplus Q(n-9) \oplus \\ Q(n-5) \oplus Q(n-4) \oplus Q(n-3)$$

(based on $P_Q(x)$ as the characteristic polynomial), where I(n) and Q(n) are binary valued ('0' and '1') and the additions are modulo-2. In order to obtain the I and Q common short-code PN sequences (of period 2^{15}), a '0' is inserted in the {I(n)} and {Q(n)} sequences after 14 consecutive '0' outputs (this occurs only once in each period). Therefore, the short-code PN sequences have one run of 15 consecutive '0' outputs instead 14. The initial state of the access terminal common short-code PN sequences, both I and Q, shall be that state in which the output of the short-code PN sequence generator is the '1' following the 15 consecutive '0' outputs.

The chip rate for the access terminal common short-code PN sequence shall be 1.2288 Mcps. The short-code PN sequence period is 32768/1228800 = 26.666... ms, and exactly 75 PN sequences repetitions occur every 2 seconds.

The access terminal shall align the I and Q short-code PN sequences such that the first chip on every even-second mark as referenced to the transmit time reference (see 9.2.1.5) is the '1' after the 15 consecutive '0's (see Figure 1.13-1).

9.2.1.3.8.2 Long Codes

The in-phase and quadrature-phase long codes, U_I and U_Q, shall be generated from a sequence, called the long-code generating sequence, by using two different masks. The long-code generating sequence shall satisfy the linear recursion specified by the following characteristic polynomial:

$$p(x) = x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} + x^{10} + x^{7} + x^{6} + x^{5} + x^{3} + x^{2} + x + 1.$$

The long codes, U_I and U_Q, shall be generated by a modulo-2 inner product of the 42-bit state vector of the sequence generator and two 42-bit masks, MI and MQ, respectively, as shown in Figure 9.2.1.3.8.2-1. The masks MI and MQ vary depending on the channel on which the access terminal is transmitting.

For transmission on the Access Channel, MI and MQ shall be set to MI_{ACMAC} and MQ_{ACMAC} (given as public data of the Access Channel MAC Protocol), respectively, and the long-code sequences are referred to as the access long codes.

For transmission on the Reverse Traffic Channel, MI and MQ shall be set to MI_{RTCMAC} and MQ_{RTCMAC} (given as public data of the Reverse Traffic Channel MAC Protocol), respectively, and the long-code sequences are referred to as the user long codes.

The long code generator shall be reloaded with the hexa-decimal value 0x24B91BFD3A8 at the beginning of every period of the short codes. Thus, the long codes are periodic with a period of 2^{15} PN chips.

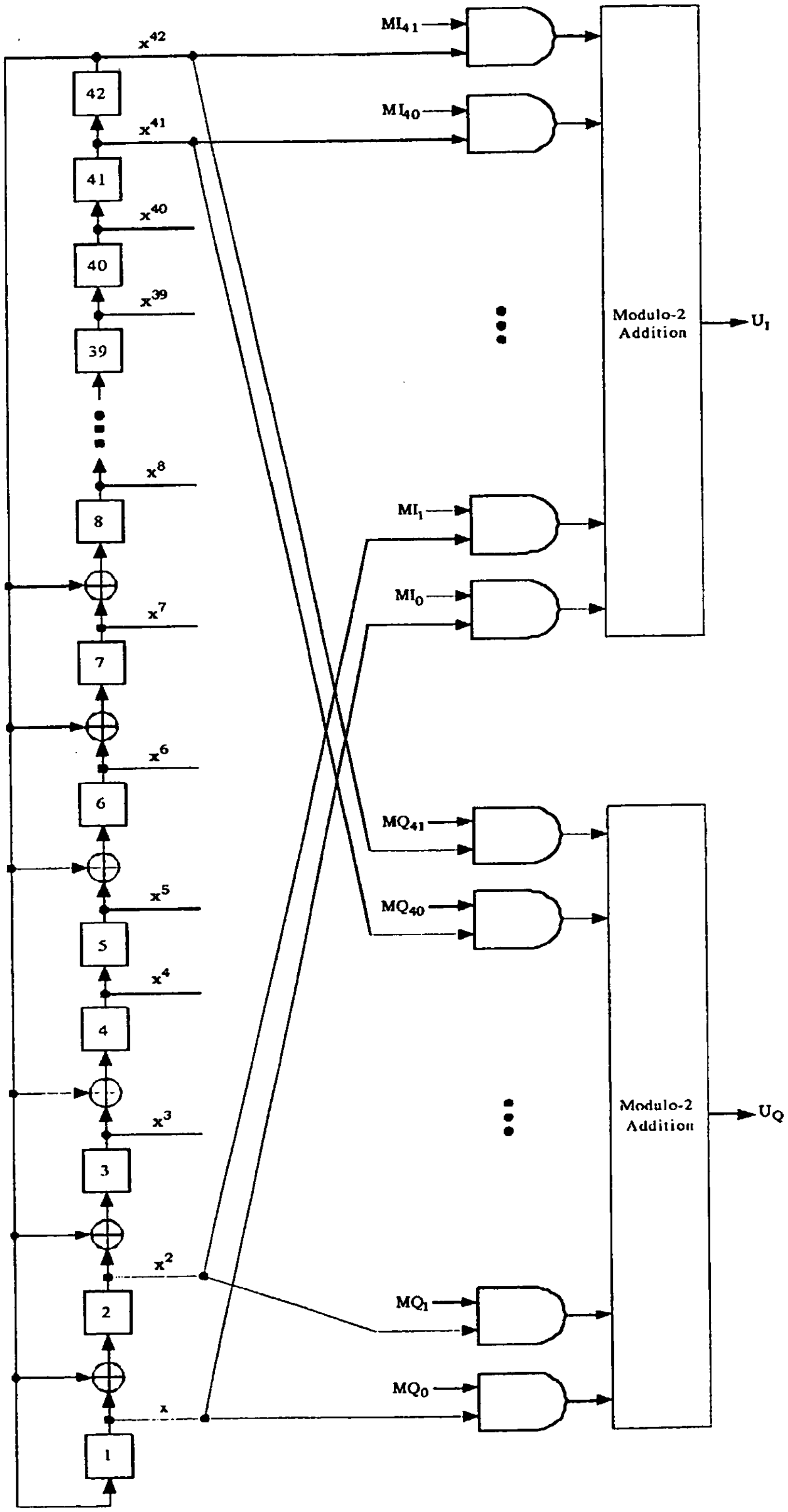


Figure 9.2.1.3.8.2-1. Long-Code Generators

9.2.1.3.8.3 Baseband Filtering

Following the quadrature spreading operation, the I' and Q' impulses are applied to the inputs of the I and Q baseband filters as shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3. The baseband filters shall have a frequency response S(f) that satisfies the limits given in Figure 9.2.1.3.8-2. Specifically, the normalized frequency response of the filter shall be contained within $\pm\delta_1$ in the passband $0 \le f \le f_p$ and shall be less than or equal to $-\delta_2$ in the stopband $f \ge f_S$. The numerical values for the parameters are δ_1 = 1.5 dB, δ_2 = 40 dB, f_p = 590 kHz, and f_S = 740 kHz.

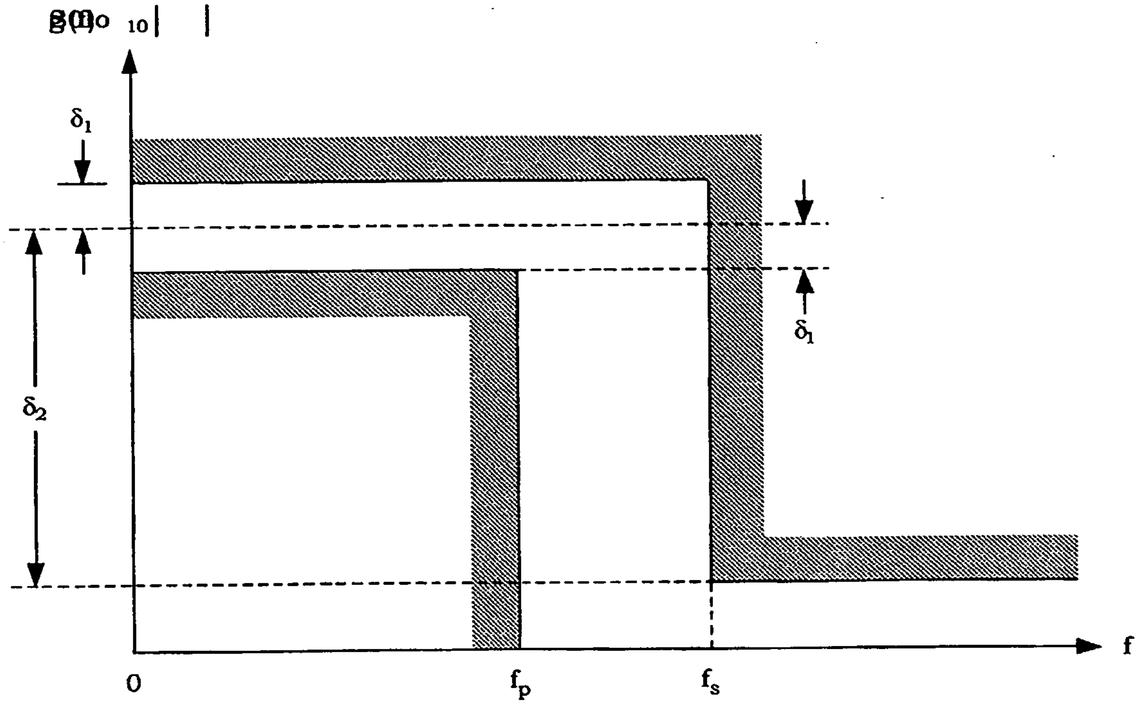


Figure 9.2.1.3.8-2. Baseband Filter Frequency Response Limits

The impulse response of the baseband filter, s(t), should satisfy the following equation:

$$\text{Mean Squared Error} = \sum_{k=0}^{\infty} [\alpha s(kT_S - \tau) - h(k)]^2 \le 0.03,$$

where the constants α and τ are used to minimize the mean squared error. The constant T_S is equal to 203.451... ns, which equals one quarter of a PN chip. The values of the coefficients h(k), for k < 48, are given in Table 9.2.1.3.8-1; h(k) = 0 for k ≥ 48. Note that h(k) equals h(47 – k).

Table 9.2.1.3.8-1. Baseband Filter Coefficients

k	h(k)
0, 47	-0.025288315
1, 46	-0.034167931
2, 45	-0.035752323
3, 44	-0.016733702
4, 43	0.021602514
5, 42	0.064938487
6, 41	0.091002137
7, 40	0.081894974
8, 39	0.037071157
9, 38	-0.021998074
10, 37	-0.060716277
11, 36	-0.051178658
12, 35	0.007874526
13, 34	0.084368728
14, 33	0.126869306
15, 32	0.094528345
16, 31	-0.012839661
17, 30	-0.143477028
18, 29	-0.211829088
19, 28	-0.140513128
20, 27	0.094601918
21, 26	0.441387140
22, 25	0.785875640
23, 24	1.0

9.2.1.4 Closed-Loop Power-Control Operation

Once the connection is established, the access network continuously transmits '0' (up) or '1' (down) RPC bits to the access terminal, based on measurements of the reverse link signal quality. If the received quality is above the target threshold, a '1' bit is transmitted. If the received quality is below the target threshold, a '0' bit is transmitted. The access terminal shall adjust its output power by a discrete amount in the direction indicated by the RPC bit after the RPC bit is received as specified in 9.2.1.2.4.2 and 9.2.1.2.5.2. The RPC bit is considered received after the 64-chip MAC burst following the second pilot burst of a slot is received as shown in Figure 9.3.1.3.1-2.

The SofterHandoff public data of the Route Update Protocol indicates whether or not two different sectors are transmitting the same RPC bit. In each slot containing power control bits, the access terminal should provide diversity combining of the identical RPC Channels and shall obtain at most one power control bit from each set of identical RPC Channels. The access terminal shall increase its output power if all the resulting RPC bits are '0' ("up"). If any resulting RPC bit is '1' ("down"), the access terminal shall decrease its output power as specified in 9.2.1.2.4.2.

9.2.1.5 Synchronization and Timing

The nominal relationship between the access terminal and access network transmit and receive time references shall be as shown in Figure 1.13-1. The access terminal shall establish a time reference that is used to derive timing for the transmitted chips, symbols, slots, frames, and system timing. The access terminal initial time reference shall be established from the acquired Pilot Channel and from the Sync message transmitted on the Control Channel. Under steady-state conditions, the access terminal time reference shall be within ±1 μs of the time of occurrence, as measured at the access terminal antenna connector, of the earliest arriving multipath component being used for demodulation. If another multipath component belonging to the same Pilot Channel or to a different Pilot Channel becomes the earliest arriving multipath component to be used, the access terminal time reference shall track to the new component. If the difference between the access terminal time reference and the time of occurrence of the earliest arriving multipath component being used for demodulation, as measured at the access terminal antenna connector, is less than ±1 μs, the access terminal may directly track its time reference to the earliest arriving multipath component being used for demodulation.

If an access terminal time reference correction is needed, it shall be corrected no faster than 203 ns (1/4 chip) in any 200-ms period and no slower than 305 ns (3/8 PN chip) per second.

The access terminal time reference shall be used as the transmit time reference of the Reverse Traffic Channel and the Access Channel.

9.3 Access Network Requirements

This section defines requirements specific to access network equipment and operation.

9.3.1 Transmitter

The transmitter shall reside in each sector of the access network. These requirements apply to the transmitter in each sector.

9.3.1.1 Frequency Parameters

9.3.1.1.1 Channel Spacing and Designation

9.3.1.1.1.1 Band Class 0 (800-MHz Band)

The Band Class 0 system designators for access network transmissions shall be as specified in Table 9.2.1.1.1.1-1. Access networks supporting Band Class 0 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.1-2 and as described in Table 9.2.1.1.1.1-3.

9.3.1.1.1.2 Band Class 1 (1900-MHz Band)

The Band Class 1 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.2-1. Access networks supporting Band Class 1 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.2-2 and as described in Table 9.2.1.1.1.2-3.

9.3.1.1.1.3 Band Class 2 (TACS Band)

The Band Class 2 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.3-1. Access networks supporting Band Class 2 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.3-3 and as described in Table 9.2.1.1.1.3-4.

9.3.1.1.1.4 Band Class 3 (JTACS Band)

The Band Class 3 system designators for access network transmissions shall be as specified in Table 9.2.1.1.1.4-1. Access networks supporting Band Class 3 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.4-2 and as described in Table 9.2.1.1.1.4-3.

9.3.1.1.1.5 Band Class 4 (Korean PCS Band)

The Band Class 4 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.5-1. Access networks supporting Band Class 4 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.5-2 and as described in Table 9.2.1.1.1.5-3.

9.3.1.1.1.6 Band Class 5 (450-MHz Band)

The Band Class 5 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.6-1. Access networks supporting Band Class 5 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.6-2 and as described in Table 9.2.1.1.1.6-3.

9.3.1.1.1.7 Band Class 6 (2-GHz Band)

The Band Class 6 block designators for access network transmissions are not specified. Access networks supporting Band Class 6 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.7-1 and as described in Table 9.2.1.1.1.7-2.

9.3.1.1.1.8 Band Class 7 (700-MHz Band)

The Band Class 7 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.8-1. Access networks supporting Band Class 7 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.8-2 and as described in Table 9.2.1.1.1.8-3.

9.3.1.1.1.9 Band Class 8 (1800-MHz Band)

The Band Class 8 block designators for access network transmissions are not specified. Access networks supporting Band Class 8 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.9-1 and as described in Table 9.2.1.1.1.9-2.

9.3.1.1.1.10 Band Class 9 (900-MHz Band)

The Band Class 9 block designators for access network transmissions are not specified. Access networks supporting Band Class 9 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.10-1 and as described in Table 9.2.1.1.1.10-2.

9.3.1.1.2 Frequency Tolerance

The average frequency difference between the actual sector transmit carrier frequency and the specified sector transmit frequency assignment shall be less than $\pm 5 \times 10^{-8}$ of the frequency assignment (±0.05 ppm).

9.3.1.2 Power Output Characteristics

The access network shall meet the requirements in the current version of [4].

9.3.1.3 Modulation Characteristics

9.3.1.3.1 Forward Channel Structure

The Forward Channel shall have the overall structure shown in Figure 9.3.1.3.1-1. The Forward Channel shall consist of the following time-multiplexed channels: the Pilot Channel, the Forward Medium Access Control (MAC) Channel, and the Forward Traffic Channel or the Control Channel. The Traffic Channel carries user physical layer packets.

The Control Channel carries control messages, and it may also carry user traffic. Each channel is further decomposed into code-division-multiplexed quadrature Walsh channels.

The forward link shall consist of slots of length 2048 chips (1.66... ms). Groups of 16 slots shall be aligned to the PN rolls of the zero-offset PN sequences and shall align to system time on even-second ticks.

Within each slot, the Pilot, MAC, and Traffic or Control Channels shall be time-division multiplexed as shown in Figure 9.3.1.3.1-2 and shall be transmitted at the same power level.

The Pilot Channel shall consist of all-'0' symbols transmitted on the I channel with Walsh cover 0. Each slot shall be divided into two half slots, each of which contains a pilot burst. Each pilot burst shall have a duration of 96 chips and be centered at the midpoint of the half slot.[45]

The MAC Channel shall consist of two subchannels: the Reverse Power Control (RPC) Channel and the Reverse Activity (RA) Channel. The RA Channel transmits a reverse link activity bit (RAB) stream.

Each MAC Channel symbol shall be BPSK modulated on one of 64 64-ary Walsh codewords (covers). The MAC symbol Walsh covers shall be transmitted four times per slot in bursts of 64 chips each. A burst shall be transmitted immediately preceding each of the pilot bursts in a slot, and a burst shall be transmitted immediately following each of the pilot bursts in a slot. The Walsh channel gains may vary the relative power.

The Forward Traffic Channel is a packet-based, variable-rate channel. The user physical layer packets for an access terminal shall be transmitted at a data rate that varies from 38.4 kbps to 2.4576 Mbps.[46]

The Forward Traffic Channel and Control Channel data shall be encoded in blocks called physical layer packets. The output of the encoder shall be scrambled and then fed into a channel interleaver. The output of the channel interleaver shall be fed into a QPSK/8-PSK/16-QAM modulator. The modulated symbol sequences shall be repeated and punctured, as necessary. Then, the resulting sequences of modulation symbols shall be demultiplexed to form 16 pairs (in-phase and quadrature) of parallel streams. Each of the parallel streams shall be covered with a distinct 16-ary Walsh function at a chip rate to yield Walsh symbols at 76.8 ksps. The Walsh-coded symbols of all the streams shall be summed together to form a single in-phase stream and a single quadrature stream at a chip rate of 1.2288 Mcps. The resulting chips are time-division multiplexed with the

[45] The pilot is used by the access terminal for initial acquisition, phase recovery, timing recovery, and maximal-ratio combining. An additional function of the pilot is to provide the access terminal with a means of predicting the receive C/I for the purpose of access-terminal-directed forward data rate control (DRC) of the Data Channel transmission.

[46] The DRC symbol from the access terminal is based primarily on its estimate of the forward C/I for the duration of the next possible forward link packet transmission.

preamble, Pilot Channel, and MAC Channel chips to form the resultant sequence of chips for the quadrature spreading operation.

Forward Traffic Channel and Control Channel physical layer packets can be transmitted in 1 to 16 slots (see Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2). When more than one slot is allocated, the transmit slots shall use a 4-slot interlacing. That is, the transmit slots of a physical layer packet shall be separated by three intervening slots, and slots of other physical layer packets shall be transmitted in the slots between those transmit slots. If a positive acknowledgement is received on the reverse link ACK Channel before all of the allocated slots have been transmitted, the remaining untransmitted slots shall not be transmitted and the next allocated slot may be used for the first slot of the next physical layer packet transmission.

Figure 9.3.1.3.1-3 and Figure 9.3.1.3.1-4 illustrate the multislot interlacing approach for a 153.6-kbps Forward Traffic Channel with DRCLength of one slot. The 153.6-kbps Forward Traffic Channel physical layer packets use four slots, and these slots are transmitted with a three-slot interval between them, as shown in the figures. The slots from other physical layer packets are interlaced in the three intervening slots. Figure 9.3.1.3.1-3 shows the case of a normal physical layer packet termination. In this case, the access terminal transmits NAK responses on the ACK Channel after the first three slots of the physical layer packet are received indicating that it was unable to correctly receive the Forward Traffic Channel physical layer packet after only one, two, or three of the nominal four slots. An ACK or NAK is also transmitted after the last slot is received, as shown. Figure 9.3.1.3.1-4 shows the case where the Forward Traffic Channel physical layer packet transmission is terminated early. In this example, the access terminal transmits an ACK response on the ACK Channel after the third slot is received indicating that it has correctly received the physical layer packet. When the access network receives such an ACK response, it does not transmit the remaining slots of the physical layer packet. Instead, it may begin transmission of any subsequent physical layer packets.

When the access network has transmitted all the slots of a physical layer packet or has received a positive ACK response, the physical layer shall return a ***ForwardTrafficCompleted*** indication.

The Control Channel shall be transmitted at a data rate of 76.8 kbps or 38.4 kbps. The modulation characteristics for the Control Channel shall be the same as those of the Forward Traffic Channel transmitted at the corresponding rate.

The Forward Traffic Channel and Control Channel data symbols shall fill the slot as shown in Figure 9.3.1.3.1-2. A slot during which no traffic or control data is transmitted is referred to as an idle slot. During an idle slot, the sector shall transmit the Pilot Channel and the MAC Channel, as described earlier.

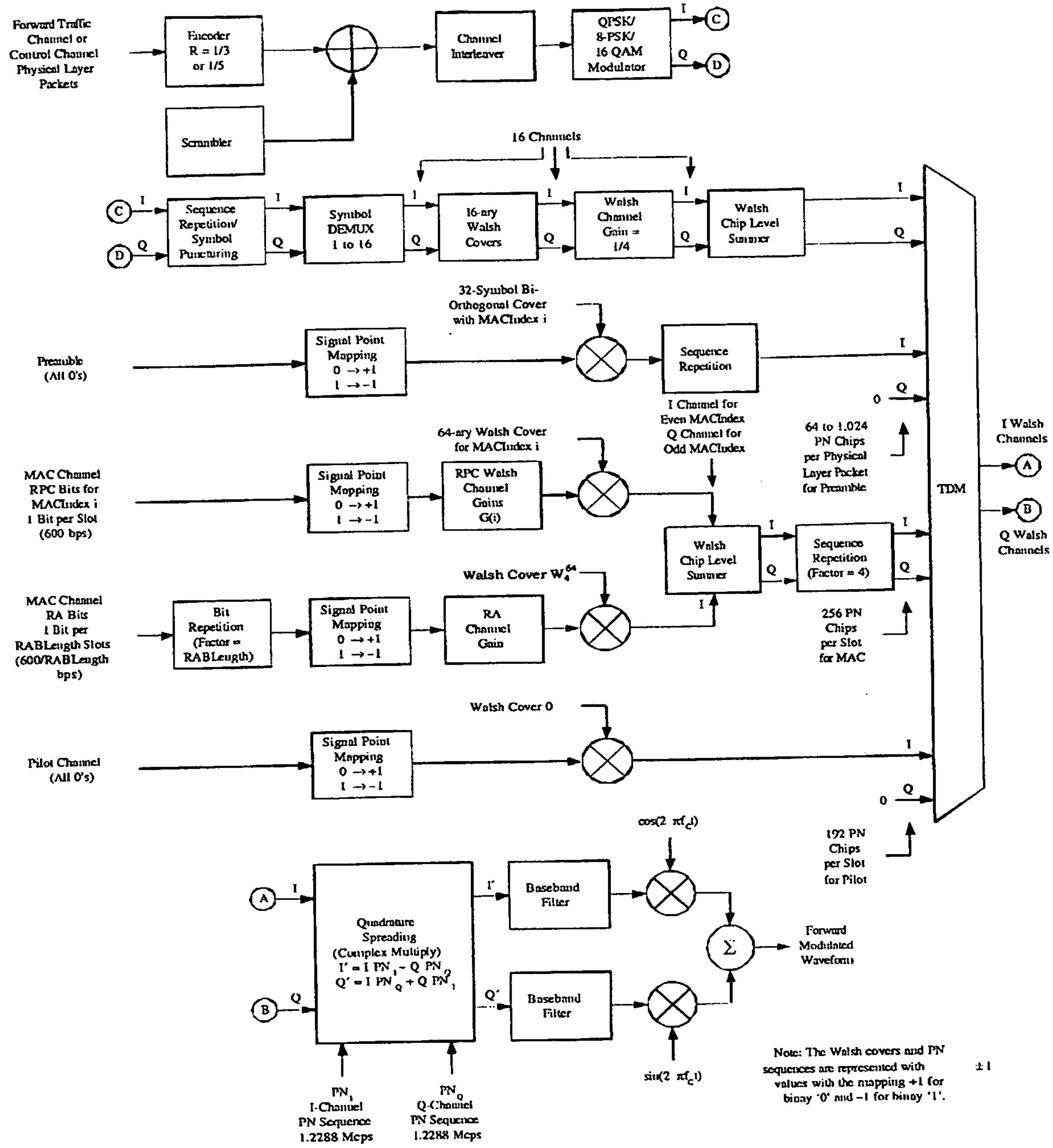

Forward Traffic Channel or Control Channel Physical Layer Packets
Encoder R = 1/3 or 1/5
Scrambler
Channel Interleaver
QPSK/ 8-PSK/ 16 QAM Modulator
I
Q
C
D
16 Channels
Sequence Repetition/ Symbol Puncturing
Symbol DEMUX 1 to 16
16-ary Walsh Covers
Walsh Channel Gain = 1/4
Walsh Chip Level Summer
32-Symbol Bi-Orthogonal Cover with MACIndex i
Preamble (All 0's)
Signal Point Mapping 0 → +1 1 → -1
Sequence Repetition
I Channel for Even MACIndex Q Channel for Odd MACIndex
0
64 to 1,024 PN Chips per Physical Layer Packet for Preamble
64-ary Walsh Cover for MACIndex i
MAC Channel RPC Bits for MACIndex i 1 Bit per Slot (600 bps)
RPC Walsh Channel Gains G(i)
TDM
I Walsh Channels
Q Walsh Channels
A
B
Walsh Chip Level Summer
Sequence Repetition (Factor = 4)
Walsh Cover W_4^{64}
MAC Channel RA Bits 1 Bit per RABLength Slots (600/RABLength bps)
Bit Repetition (Factor = RABLength)
RA Channel Gain
256 PN Chips per Slot for MAC
Walsh Cover 0
Pilot Channel (All 0's)
192 PN Chips per Slot for Pilot
$\cos(2\pi f_c t)$
Quadrature Spreading (Complex Multiply) $I' = I\ PN_I - Q\ PN_Q$ $Q' = I\ PN_Q + Q\ PN_I$
I'
Q'
Baseband Filter
Baseband Filter
Σ
Forward Modulated Waveform
$\sin(2\pi f_c t)$
PN_I I-Channel PN Sequence 1.2288 Mcps
PN_Q Q-Channel PN Sequence 1.2288 Mcps
Note: The Walsh covers and PN sequences are represented with ±1 values with the mapping +1 for binay '0' and -1 for binay '1'.

Figure 9.3.1.3.1-1. Forward Channel Structure

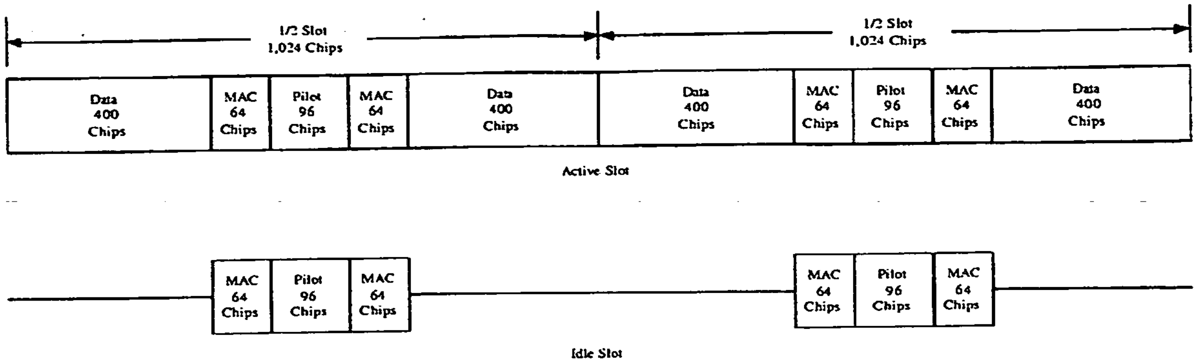


Figure 9.3.1.3.1-2. Forward Link Slot Structure

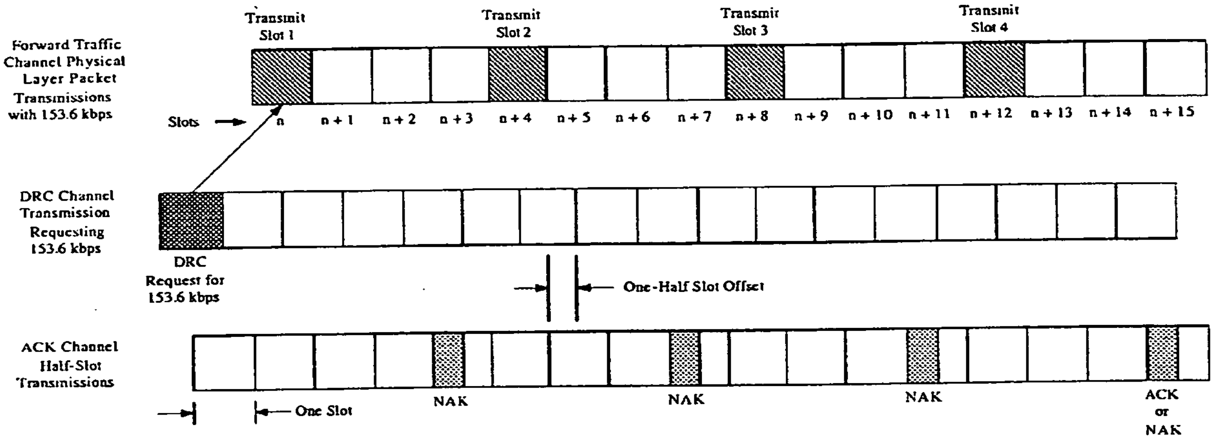


Figure 9.3.1.3.1-3. Multislot Physical Layer Packet with Normal Termination

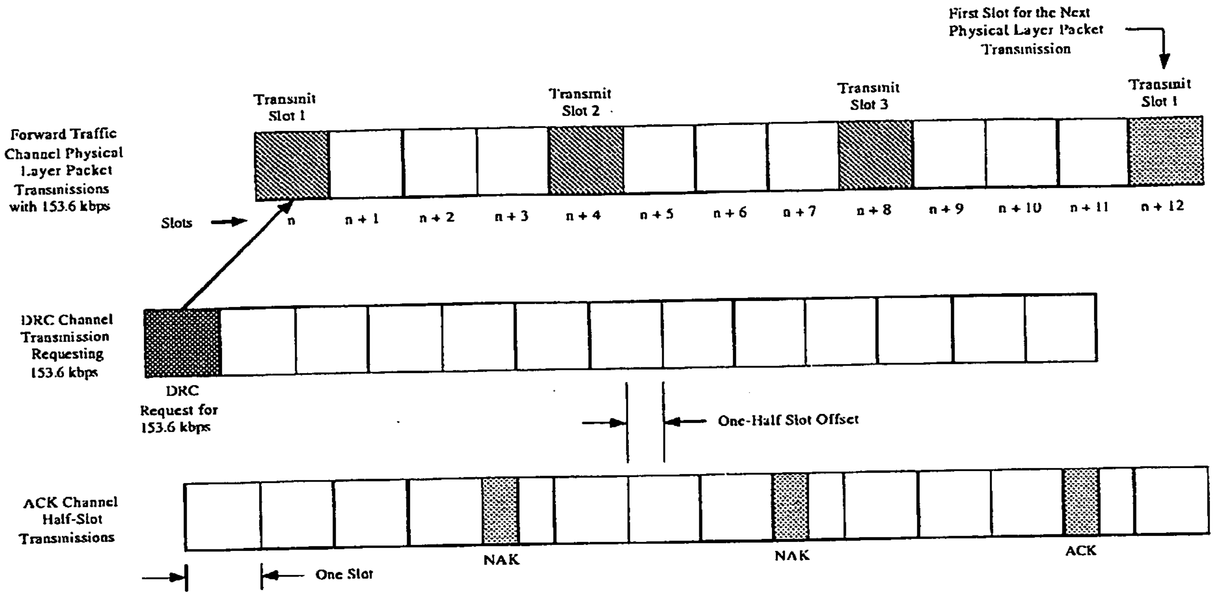

First Slot for the Next Physical Layer Packet Transmission
Transmit Slot 1
Transmit Slot 2
Transmit Slot 3
Transmit Slot 1
Forward Traffic Channel Physical Layer Packet Transmissions with 153.6 kbps
Slots
n
n + 1
n + 2
n + 3
n + 4
n + 5
n + 6
n + 7
n + 8
n + 9
n + 10
n + 11
n + 12
DRC Channel Transmission Requesting 153.6 kbps
DRC Request for 153.6 kbps
One-Half Slot Offset
ACK Channel Half-Slot Transmissions
NAK
NAK
ACK
One Slot

Figure 9.3.1.3.1-4. Multislot Physical Layer Packet with Early Termination

9.3.1.3.1.1 Modulation Parameters

The modulation parameters for the Forward Traffic Channel and the Control Channel shall be as shown in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2. The Control Channel shall only use the 76.8 kbps and 38.4 kbps data rates.

Table 9.3.1.3.1.1-1. Modulation Parameters for the Forward Traffic Channel and the Control Channel (Part 1 of 2)

Data Rate (kbps)	Number of Values per Physical Layer Packet				
	Slots	Bits	Code Rate	Modulation Type	TDM Chips (Preamble, Pilot, MAC, Data)
38.4	16	1,024	1/5	QPSK	1,024 3,072 4,096 24,576
76.8	8	1,024	1/5	QPSK	512 1,536 2,048 12,288
153.6	4	1,024	1/5	QPSK	256 768 1,024 6,144
307.2	2	1,024	1/5	QPSK	128 384 512 3,072
614.4	1	1,024	1/3	QPSK	64 192 256 1,536

Table 9.3.1.3.1.1-2. Modulation Parameters for the Forward Traffic Channel and the Control Channel (Part 2 of 2)

Data Rate (kbps)	Number of Values per Physical Layer Packet				
	Slots	Bits	Code Rate	Modulation Type	TDM Chips (Preamble, Pilot, MAC, Data)
307.2	4	2,048	1/3	QPSK	128 768 1,024 6,272
614.4	2	2,048	1/3	QPSK	64 384 512 3,136
1,228.8	1	2,048	1/3	QPSK	64 192 256 1,536
921.6	2	3,072	1/3	8-PSK	64 384 512 3,136
1,843.2	1	3,072	1/3	8-PSK	64 192 256 1,536
1,228.8	2	4,096	1/3	16-QAM	64 384 512 3,136
2,457.6	1	4,096	1/3	16-QAM	64 192 256 1,536

The modulation parameters for the MAC Channel shall be as shown in Table 9.3.1.3.1.1-3.

Table 9.3.1.3.1.1-3. Modulation Parameters for the MAC Channel

Parameter	RPC Channel	RA Channel
Rate (bps)	600	600/RABLength
Bit Repetition Factor	1	RABLength
Modulation (Channel)	BPSK (I or Q)	BPSK (I)
Modulation Symbol Rate (sps)	2,400	2,400
Walsh Cover Length	64	64
Walsh Sequence Repetition Factor	4	4
PN Chips/Slot	256	256
PN Chips/Bit	256	256 × RABLength

9.3.1.3.1.2 Data Rates

The Forward Traffic Channel shall support variable-data-rate transmission from 38.4 kbps to 2.4576 Mbps, as shown in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2.

The data rate of the Control Channel shall be 76.8 kbps or 38.4 kbps.

9.3.1.3.2 Forward Link Channels

9.3.1.3.2.1 Pilot Channel

A Pilot Channel shall be transmitted at all times by the sector on each active Forward Channel. The Pilot Channel is an unmodulated signal that is used for synchronization and other functions by an access terminal operating within the coverage area of the sector. The Pilot Channel shall be transmitted at the full sector power.

9.3.1.3.2.1.1 Modulation

The Pilot Channel shall consist of all-'0' symbols transmitted on the I component only.

9.3.1.3.2.1.2 Orthogonal Spreading

The Pilot Channel shall be assigned Walsh cover 0.

9.3.1.3.2.1.3 Quadrature Spreading

See 9.3.1.3.4.

9.3.1.3.2.2 Forward MAC Channel

The Forward MAC Channel shall be composed of Walsh channels that are orthogonally covered and BPSK modulated on a particular phase of the carrier (either in-phase or quadrature phase). Each Walsh channel shall be identified by a MACIndex value that is between 0 and 63 and defines a unique 64-ary Walsh cover and a unique modulation phase. The Walsh functions assigned to the MACIndex values shall be as follows:

$$W^{64}_{i/2} = 0, 2, \ldots, 62$$

$$W^{64}_{(i-1)/2+32} = 1, 3, \ldots, 63$$

where i is the MACIndex value. MAC Channels with even-numbered MACIndex values shall be assigned to the in-phase (I) modulation phase, while those with odd-numbered MACIndex values shall be assigned to the quadrature (Q) modulation phase. The MAC symbol Walsh covers shall be transmitted four times per slot in bursts of length 64 chips each. These bursts shall be transmitted immediately preceding and following the pilot bursts of each slot.

The MAC Channel use versus MACIndex shall be as specified in Table 9.3.1.3.2.1.3-1.

Symbols of each MAC Channel shall be transmitted on one of the Walsh channels. The MAC channel gains may vary the relative power as a function of time. The orthogonal Walsh channels shall be scaled to maintain a constant total transmit power. The sum of the squares of the normalized gains on the orthogonal MAC Channels should equal one. The Walsh Channel gains can vary as a function of time.

Table 9.3.1.3.2.1.3-1. MAC Channel and Preamble Use Versus MACIndex

MACIndex	MAC Channel Use	Preamble Use
0 and 1	Not Used	Not Used
2	Not Used	76.8-kbps Control Channel
3	Not Used	38.4-kbps Control Channel
4	RA Channel	Not Used
5–63	Available for RPC Channel Transmissions	Available for Forward Traffic Channel Transmissions

9.3.1.3.2.2.1 Reverse Power Control Channel

The Reverse Power Control (RPC) Channel for each access terminal with an open connection shall be assigned to one of the available MAC Channels. It is used for the transmission of the RPC bit stream destined to that access terminal.

The RPC data rate shall be 600 bps. Each RPC symbol shall be transmitted four times per slot in bursts of 64 chips each. One burst shall be transmitted immediately preceding and following each pilot burst in a slot as shown in Figure 9.3.1.3.1-2.

9.3.1.3.2.2.2 Reverse Activity Channel

The Reverse Activity (RA) Channel shall transmit the Reverse Activity Bit (RAB) stream over the MAC Channel with MACIndex 4. The RA bit shall be transmitted over RABLength successive slots. The transmission of each RA bit shall start in a slot that satisfies

$$T \bmod \text{RABLength} = \text{RABOffset},$$

where T is the system time in slots and RABLength and RABOffset are fields in the public data TrafficChannelAssignment of the Route Update Protocol.

The RA Channel data rate shall be 600/RABLength bps. Each RA bit shall be repeated and transmitted over RABLength consecutive slots. The RA bit in each slot shall be further repeated to form four symbols per slot for transmission.

9.3.1.3.2.3 Forward Traffic Channel

9.3.1.3.2.3.1 Forward Traffic Channel Preamble

A preamble sequence shall be transmitted with each Forward Traffic Channel and Control Channel physical layer packet in order to assist the access terminal with synchronization of each variable-rate transmission.

The preamble shall consist of all-'0' symbols transmitted on the in-phase component only. The preamble shall be time multiplexed into the Forward Traffic Channel stream as described in 9.3.1.3.3. The preamble sequence shall be covered by a 32-chip bi-orthogonal sequence and the sequence shall be repeated several times depending on the transmit mode. The bi-orthogonal sequence shall be specified in terms of the 32-ary Walsh functions and their bit-by-bit complements by

$$W_{i/2}^{32}, \; i = 0, 2, \ldots, 62$$
$$\overline{W_{(i-1)/2}^{32}}, \; i = 1, 3, \ldots, 63$$

where i = 0, 1,..., 63 is the MACIndex value and $\overline{W_i^{32}}$ is the bit-by-bit complement of the 32-chip Walsh function of order i.

The channel type versus MACIndex mapping for the preamble shall be as specified in Table 9.3.1.3.2.1.3-1.

The 32-chip preamble repetition factor shall be as specified in Table 9.3.1.3.2.3.1-1.

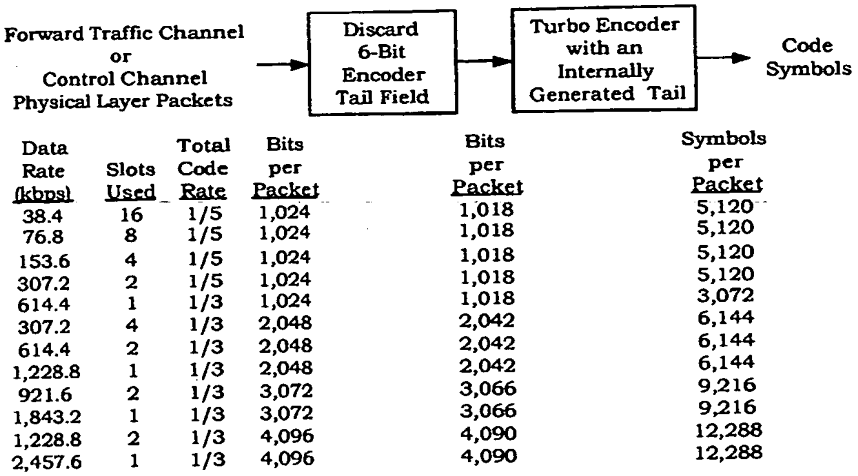
Table 9.3.1.3.2.3.1-1. Preamble Repetition

Data Rate (kbps)	Values per Physical Layer Packet		
	Slots	32-Chip Preamble Sequence Repetitions	Preamble Chips
38.4	16	32	1,024
76.8	8	16	512
153.6	4	8	256
307.2	2	4	128
614.4	1	2	64
307.2	4	4	128
614.4	2	2	64
1,228.8	1	2	64
921.6	2	2	64
1,843.2	1	2	64
1,228.8	2	2	64
2,457.6	1	2	64

9.3.1.3.2.3.2 Encoding

The Traffic Channel physical layer packets shall be encoded with code rates of R = 1/3 or 1/5. The encoder shall discard the 6-bit TAIL field of the physical layer packet inputs and encode the remaining bits with a parallel turbo encoder, as specified in 9.3.1.3.2.3.2.1. The turbo encoder will add an internally generated tail of 6/R output code symbols, so that the total number of output symbols is 1/R times the number of bits in the input physical layer packet.

Figure 9.3.1.3.2.3.2-1 illustrates the forward link encoding approach. The forward link encoder parameters shall be as specified in Table 9.3.1.3.2.3.2-1.



Data Rate (kbps)	Slots Used	Total Code Rate	Bits per Packet	Bits per Packet	Symbols per Packet
38.4	16	1/5	1,024	1,018	5,120
76.8	8	1/5	1,024	1,018	5,120
153.6	4	1/5	1,024	1,018	5,120
307.2	2	1/5	1,024	1,018	5,120
614.4	1	1/3	1,024	1,018	3,072
307.2	4	1/3	2,048	2,042	6,144
614.4	2	1/3	2,048	2,042	6,144
1,228.8	1	1/3	2,048	2,042	6,144
921.6	2	1/3	3,072	3,066	9,216
1,843.2	1	1/3	3,072	3,066	9,216
1,228.8	2	1/3	4,096	4,090	12,288
2,457.6	1	1/3	4,096	4,090	12,288

Figure 9.3.1.3.2.3.2-1. Forward Link Encoder

Table 9.3.1.3.2.3.2-1. Parameters of the Forward Link Encoder

Data Rate (kbps)	Values per Physical Layer Packet				
	Slots	Bits	Turbo Encoder Input Bits	Code Rate	Turbo Encoder Output Symbols
38.4	16	1,024	1,018	1/5	5,120
76.8	8	1,024	1,018	1/5	5,120
153.6	4	1,024	1,018	1/5	5,120
307.2	2	1,024	1,018	1/5	5,120
614.4	1	1,024	1,018	1/3	3,072
307.2	4	2,048	2,042	1/3	6,144
614.4	2	2,048	2,042	1/3	6,144
1,228.8	1	2,048	2,042	1/3	6,144
921.6	2	3,072	3,066	1/3	9,216
1,843.2	1	3,072	3,066	1/3	9,216
1,228.8	2	4,096	4,090	1/3	12,288
2,457.6	1	4,096	4,090	1/3	12,288

9.3.1.3.2.3.2.1 Turbo Encoder

The turbo encoder employs two systematic, recursive, convolutional encoders connected in parallel, with an interleaver, the turbo interleaver, preceding the second recursive convolutional encoder. The two recursive convolutional codes are called the constituent codes of the turbo code. The outputs of the constituent encoders are punctured and repeated to achieve the desired number of turbo encoder output symbols.

The transfer function for the constituent code shall be

$$G(D) = \left[\quad \frac{n_0(D)}{d(D)} \quad \frac{n_1(D)}{} \right]$$

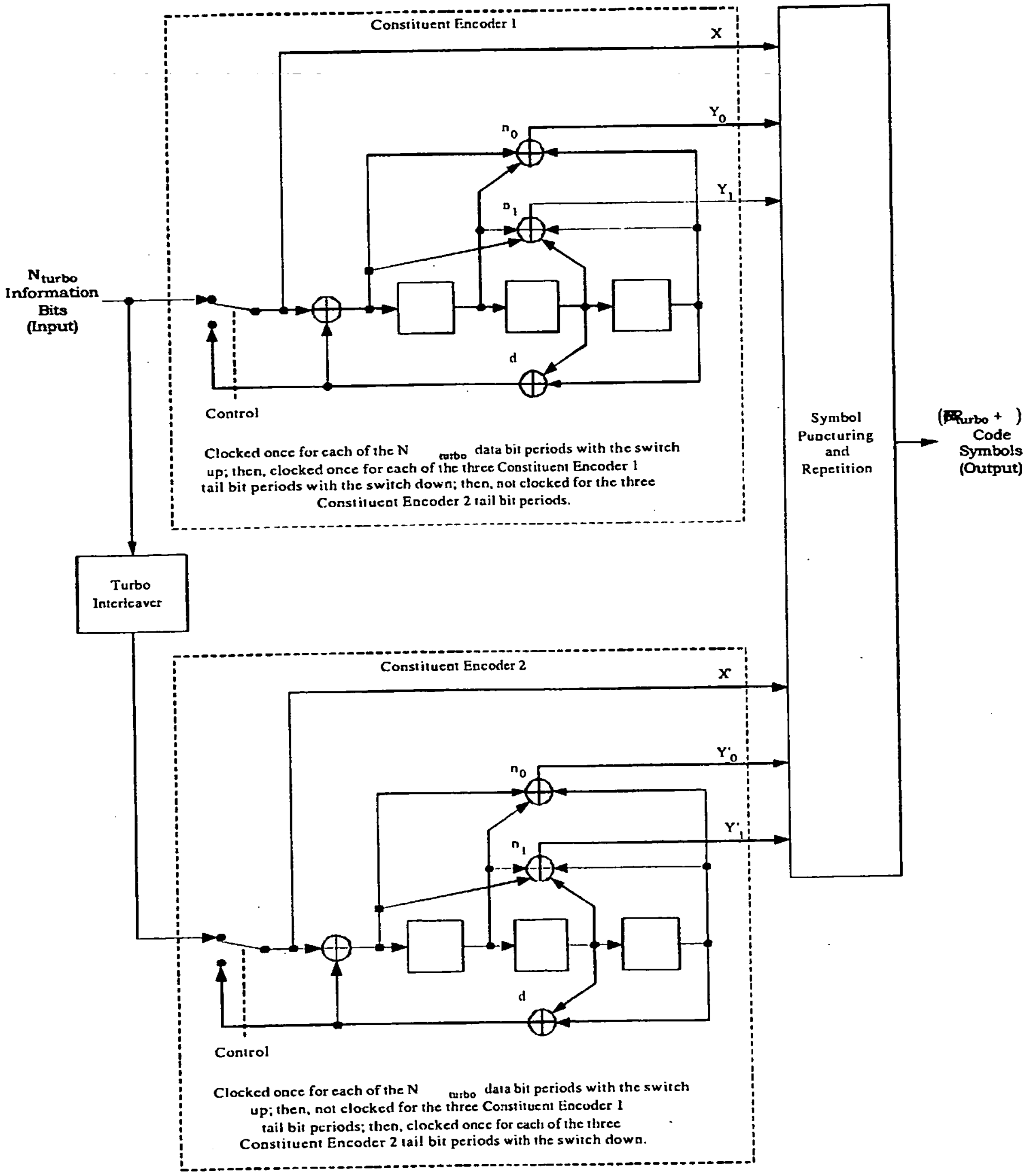
where $d(D) = 1 + D^2 + D^3$, $n_0(D) = 1 + D + D^3$, and $n_1(D) = 1 + D + D^2 + D^3$.

The turbo encoder shall generate an output symbol sequence that is identical to the one generated by the encoder shown in Figure 9.3.1.3.2.3.2.1-1. Initially, the states of the constituent encoder registers in this figure are set to zero. Then, the constituent encoders are clocked with the switches in the positions noted.

Let N_{turbo} be the number of bits into the turbo encoder after the 6-bit physical layer packet TAIL field is discarded. Then, the encoded data output symbols are generated by clocking Nhe constituent encoders $_{turbo}$ times with the switches in the up positions and puncturing the outputs as specified in Table 9.3.1.3.2.3.2.1-1. Within a puncturing pattern, a '0' means that the symbol shall be deleted and a '1' means that the symbol shall be passed. The constituent encoder outputs for each bit period shall be output in the sequence X, Y_0, Y_1, X′, Y'_0, Y'_1 with the X output first. Symbol repetition is not used in generating the encoded data output symbols.

The turbo encoder shall generate 6/R tail output symbols following the encoded data output symbols. This tail output symbol sequence shall be identical to the one generated by the encoder shown in Figure 9.3.1.3.2.3.2.1-1. The tail output symbols are generated after the constituent encoders have been clocked N_{turbo} times with the switches in the up position. The first 3/R tail output symbols are generated by clocking Constituent Encoder 1 three times with its switch in the down position while Constituent Encoder 2 is not clocked and puncturing and repeating the resulting constituent encoder output symbols. The last 3/R tail output symbols are generated by clocking Constituent Encoder 2 three times with its switch in the down position while Constituent Encoder 1 is not clocked and puncturing and repeating the resulting constituent encoder output symbols. The constituent encoder outputs for each bit period shall be output in the sequence X, Y_0, Y_1, X′, Y'_0, Y'_1 with the X output first.

The constituent encoder output symbol puncturing for the tail symbols shall be as specified in Table 9.3.1.3.2.3.2.1-2. Within a puncturing pattern, a '0' means that the symbol shall be deleted and a '1' means that a symbol shall be passed. For rate-1/5 turbo codes, the tail output code symbols for each of the first three tail bit periods shall be punctured and repeated to achieve the sequence $XXY_0Y_1Y_1$, and the tail output code symbols for each of the last three tail bit periods shall be punctured and repeated to achieve the sequence $X'X'Y'_0Y'_1Y'_1$. For rate-1/3 turbo codes, the tail output symbols for each of the first three tail bit periods shall be XXY_0, and the tail output symbols for each of the last three tail bit periods shall be $X'X'Y'_0$.



Clocked once for each of the N_{turbo} data bit periods with the switch up; then, clocked once for each of the three Constituent Encoder 1 tail bit periods with the switch down; then, not clocked for the three Constituent Encoder 2 tail bit periods.

Clocked once for each of the N_{turbo} data bit periods with the switch up; then, not clocked for the three Constituent Encoder 1 tail bit periods; then, clocked once for each of the three Constituent Encoder 2 tail bit periods with the switch down.

Figure 9.3.1.3.2.3.2.1-1. Turbo Encoder

Table 9.3.1.3.2.3.2.1-1. Puncturing Patterns for the Data Bit Periods

	Code Rate	
Output	1/3	1/5
X	1	1
Y_0	1	1
Y_1	0	1
X′	0	0
Y'_0	1	1
Y'_1	0	1

Note: For each rate, the puncturing table shall be read from top to bottom.

Table 9.3.1.3.2.3.2.1-2. Puncturing Patterns for the Tail Bit Periods

	Code Rate	
Output	1/3	1/5
X	111 000	111 000
Y_0	111 000	111 000
Y_1	000 000	111 000
X′	000 111	000 111
Y'_0	000 111	000 111
Y'_1	000 000	000 111

Note: For rate-1/3 turbo codes, the puncturing table shall be read first from top to bottom repeating X and X′, and then from left to right. For rate-1/5 turbo codes, the puncturing table shall be read first from top to bottom repeating X, X′, Y_1, and Y'_1 and then from left to right.

9.3.1.3.2.3.2.2 Turbo Interleaver

The turbo interleaver, which is part of the turbo encoder, shall block interleave the turbo encoder input data that is fed to Constituent Encoder 2.

The turbo interleaver shall be functionally equivalent to an approach where the entire aequence of turbo interleaver input bits are written sequentially into an array at sequence of addresses, and then the entire sequence is read out from a sequence of addresses that are defined by the procedure described below.

Let the sequence of input addresses be from 0 to N_{turbo} – 1. Then, the sequence of interleaver output addresses shall be equivalent to those generated by the procedure illustrated in Figure 9.3.1.3.2.3.2.2-1 and described below.[47]

1. Determine the turbo interleaver parameter, n, where n is the smallest integer such that $N_{turbo} \le 2^{n+5}$. Table 9.3.1.3.2.3.2.2-1 gives this parameter for the different physical layer packet sizes.
2. Initialize an (n + 5)-bit counter to 0.
3. Extract the n most significant bits (MSBs) from the counter and add one to form a new value. Then, discard all except the n least significant bits (LSBs) of this value.
4. Obtain the n-bit output of the table lookup defined in Table 9.3.1.3.2.3.2.2-2 with a read address equal to the five LSBs of the counter. Note that this table depends on the value of n.
5. Multiply the values obtained in Steps 3 and 4, and discard all except the n LSBs.
6. Bit-reverse the five LSBs of the counter.
7. Form a tentative output address that has its MSBs equal to the value obtained in Step 6 and its LSBs equal to the value obtained in Step 5.
8. Accept the tentative output address as an output address if it is less than N_{turbo}; otherwise, discard it.
9. Increment the counter and repeat Steps 3 through 8 until all N_{turbo} interleaver output addresses are obtained.

[47] This procedure is equivalent to one where the counter values are written into a 2^5-row by 2^n-column array by rows, the rows are shuffled according to a bit-reversal rule, the elements within each row are permuted according to a row-specific linear congruential sequence, and tentative output addresses are read out by column. The linear congru ntial sequence rule is $x(i + 1) = (x(i) + c) \bmod 2^n$, where $x(0) = c$ and c is a row-specific value from a table lookup.

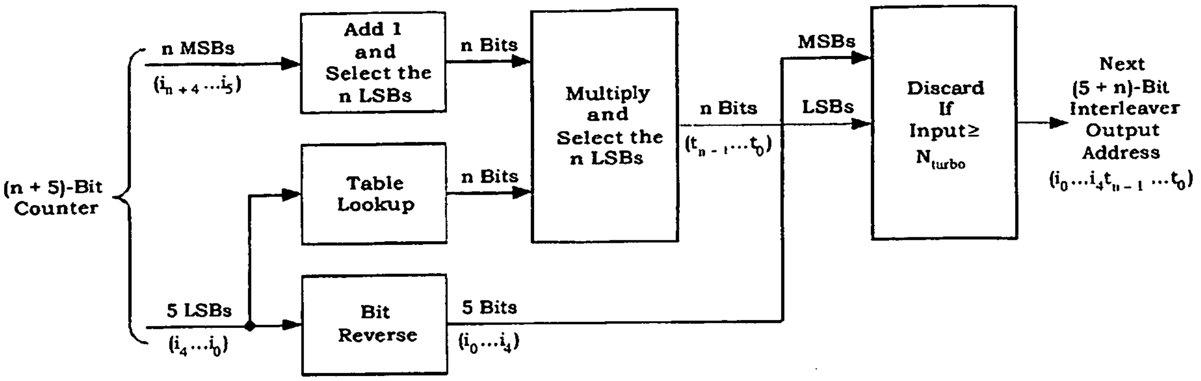


Figure 9.3.1.3.2.3.2.2-1. Turbo Interleaver Output Address Calculation Procedure

Table 9.3.1.3.2.3.2.2-1. Turbo Interleaver Parameter

Physical Layer Packet Size	Turbo Interleaver Block Size N_{turbo}	Turbo Interleaver Parameter n
1,024	1,018	5
2,048	2,042	6
3,072	3,066	7
4,096	4,090	7

Table 9.3.1.3.2.3.2.2-2. Turbo Interleaver Lookup Table Definition

Table Index	n = 5 Entries	n = 6 Entries	n = 7 Entries
0	27	3	15
1	3	27	127
2	1	15	89
3	15	13	1
4	13	29	31
5	17	5	15
6	23	1	61
7	13	31	47
8	9	3	127
9	3	9	17
10	15	15	119
11	3	31	15
12	13	17	57
13	1	5	123
14	13	39	95
15	29	1	5
16	21	19	85
17	19	27	17
18	1	15	55
19	3	13	57
20	29	45	15
21	17	5	41
22	25	33	93
23	29	15	87
24	9	13	63
25	13	9	15
26	23	15	13
27	13	31	15
28	13	17	81
29	1	5	57
30	13	15	31
31	13	33	69

9.3.1.3.2.3.3 Scrambling

The output of the encoder shall be scrambled to randomize the data prior to modulation. The scrambling sequence shall be equivalent to one generated with a 17-tap linear feedback shift register with a generator sequence of $h(D) = D^{17} + D^{14} + 1$, as shown in Figure 9.3.1.3.2.3.3-1. At the start of the physical layer packet, the shift register shall be initialized to the state $[1111111r_5r_4r_3r_2r_1r_0d_3d_2d_1d_0]$. The $r_5r_4r_3r_2r_1r_0$ bits shall be equal to the 6-bit preamble MACIndex value (see Table 9.3.1.3.2.1.3-1). The $d_3d_2d_1d_0$ bits shall be determined by the data rate, as specified in Table 9.3.1.3.2.3.3-1. The initial state shall generate the first scrambling bit. The shift register shall be clocked once for every encoder output code symbol to generate a bit of the scrambling sequence. Every encoder output code symbol shall be XOR'd with the corresponding bit of the scrambling sequence to yield a scrambled encoded bit.

Table 9.3.1.3.2.3.3-1. Parameters Controlling the Scrambler Initial State

Data Rate (kbps)	Slots per Physical Layer Packet	d_3	d_2	d_1	d_0
38.4	16	0	0	0	1
76.8	8	0	0	1	0
153.6	4	0	0	1	1
307.2	2	0	1	0	0
307.2	4	0	1	0	1
614.4	1	0	1	1	0
614.4	2	0	1	1	1
921.6	2	1	0	0	0
1,228.8	1	1	0	0	1
1,228.8	2	1	0	1	0
1,843.2	1	1	0	1	1
2,457.6	1	1	1	0	0

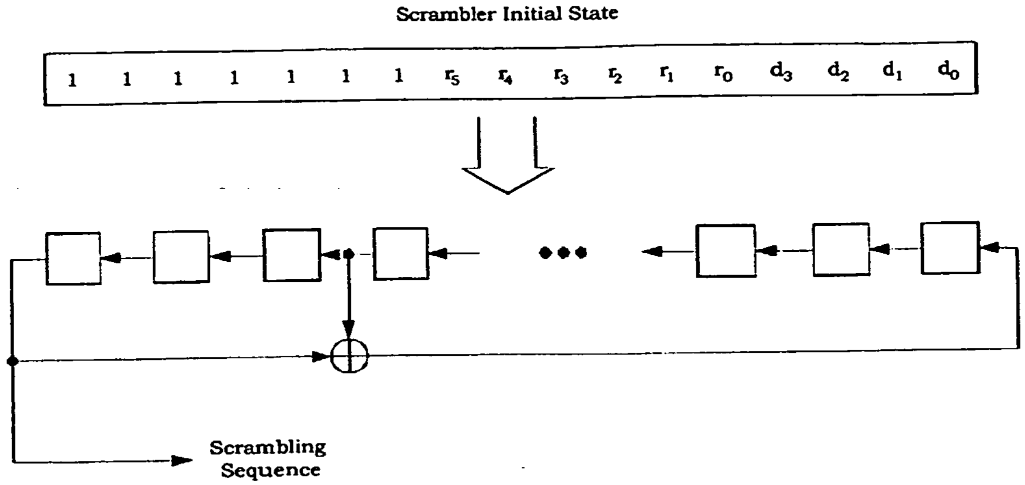


Figure 9.3.1.3.2.3.3-1. Symbol Scrambler

9.3.1.3.2.3.4 Channel Interleaving

The channel interleaving shall consist of a symbol reordering followed by symbol permuting.

9.3.1.3.2.3.4.1 Symbol Reordering

The scrambled turbo encoder data and tail output symbols generated with the rate-1/5 encoder shall be reordered according to the following procedure:

1. All of the scrambled data and tail turbo encoder output symbols shall be demultiplexed into five sequences denoted U, V_0, V_1, V'_0, and V'_1. The scrambled encoder output symbols shall be sequentially distributed from the U sequence to the V'_1 sequence with the first scrambled encoder output symbol going to the U sequence, the second to the V_0 sequence, the third to the V_1 sequence, the fourth to the V'_0 sequence, the fifth to the V'_1 sequence, the sixth to the U sequence, etc.
2. The U, V_0, V_1, V'_0, and V'_1 sequences shall be ordered according to $UV_0V'_0V_1V'_1$. That is, the U sequence of symbols shall be first and the V'_1 sequence of symbols shall be last.

The scrambled turbo encoder data and tail output symbols generated with the rate-1/3 encoder shall be reordered according to the following procedure:

1. All of the scrambled data and tail turbo encoder output symbols shall be demultiplexed into three sequences denoted U, V_0, and V'_0. The scrambled encoder output symbols shall be sequentially distributed from the U sequence to the V'_0 sequence with the first scrambled encoder output symbol going to the U sequence, the second to the V_0 sequence, the third to the V'_0 sequence, the fourth to the U sequence, etc.

2. The U, V_0, and V'_0 sequences shall be ordered according to $UV_0V'_0$. That is, the U sequence of symbols shall be first and the V'_0 sequence of symbols shall be last.

Table 9.3.1.3.2.3.4.1-1 gives the order of the symbols out of the turbo encoder and their mapping to demultiplexer output sequences. The encoder output symbol notation is used, but the encoder output symbols are scrambled before the reordering demultiplexer.

Table 9.3.1.3.2.3.4.1-1. Scrambled Turbo Encoder Output and Symbol Reordering Demultiplexer Symbol Sequences

Type of Sequence	Symbol Sequence	
	R = 1/5	R = 1/3
Turbo Encoder Data Output Sequence	$X\,Y_0\,Y_1\,Y'_0\,Y'_1$	$X\,Y_0\,Y'_0$
Turbo Encoder Constituent Encoder 1 Tail Output Sequence	$X\,X\,Y_0\,Y_1\,Y_1$	$X\,X\,Y_0$
Turbo Encoder Constituent Encoder 2 Tail Output Sequence	$X'\,X'\,Y'_0\,Y'_1\,Y'_1$	$X'\,X'\,Y'_0$
Demultiplexer Output Sequence	$U\,V_0\,V'_0\,V_1\,V'_1$	$U\,V_0\,V'_0$

9.3.1.3.2.3.4.2 Symbol Permuting

The reordered symbols shall be permuted in three separate bit-reversal interleaver blocks with rate-1/5 coding and in two separate blocks with rate-1/3 coding. The permuter input blocks shall consist of the sequence of U symbols, the sequence of V_0 and V_0 symbols (denoted as V_0/V'_0), and, with rate-1/5 coding, the sequence of V_1 and V'_1 symbols (denoted as V_1/V'_1).

The sequence of interleaver output symbols for the blocks shall be equivalent to those generated by the procedure described below with the parameters specified in Table 9.3.1.3.2.3.4.2-1:

1. Write the entire sequence of symbols in the input block into a rectangular array of K rows and M columns. Write the symbols in by rows starting from the top row, writing the rows from left to right.

2. Label the columns of the array by the index j, where j = 0,..., M − 1 and column 0 is the left-most column. Then, end-around shift the symbols of each column downward by j mod K for the U block and by $\lfloor j/4 \rfloor$ mod K for the V_0/V'_0 and V_1/V'_1 blocks.

3. Reorder the columns such that column j is moved to column BRO(j), where BRO(j) indicates the bit-reversed value of j. For example, for M = 512, BRO(6) = 192.

4. Read the entire array of symbols out by columns starting from the left-most column, reading the columns from top to bottom.

With rate-1/5 coding, the interleaver output sequence shall be the interleaved U symbols followed by the interleaved V_0/V'_0 symbols followed by the interleaved V_1/V'_1 symbols. With rate-1/3 coding, the interleaver output sequence shall be the interleaved U symbols followed by the interleaved V_0/V'_0.

Table 9.3.1.3.2.3.4.2-1. Channel Interleaver Parameters

Physical Layer Packet Size	U Block Interleaver Parameters		V_0/V'_0 and V_1/V'_1 Block Interleaver Parameters	
	K	M	K	M
1,024	2	512	2	1,024
2,048	2	1,024	2	2,048
3,072	3	1,024	3	2,048
4,096	4	1,024	4	2,048

9.3.1.3.2.3.5 Modulation

The output of the channel interleaver shall be applied to a modulator that outputs an in-phase stream and a quadrature stream of modulated values. The modulator generates QPSK, 8-PSK, or 16-QAM modulation symbols, depending on the data rate.

9.3.1.3.2.3.5.1 QPSK Modulation

For physical layer packet sizes of 1,024 or 2,048 bits, groups of two successive channel interleaver output symbols shall be grouped to form QPSK modulation symbols. Each group of two adjacent block interleaver output symbols, x(2i) and x(2i + 1), i = 0,..., M – 1 as specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol $(m_I(i), m_Q(i))$ as specified in Table 9.3.1.3.2.3.5.1-1. Figure 9.3.1.3.2.3.5.1-1 shows the signal constellation of the QPSK modulator, where $s_0 = x(2k)$ and $s_1 = x(2k + 1)$.

Table 9.3.1.3.2.3.5.1-1. QPSK Modulation Table

Interleaved Symbols		Modulation Symbols	
s_1 x(2k + 1)	s_0 x(2k)	$m_I(k)$	$m_Q(k)$
0	0	D	D
0	1	–D	D
1	0	D	–D
1	1	–D	–D

Note: $D = 1/\sqrt{2}$.

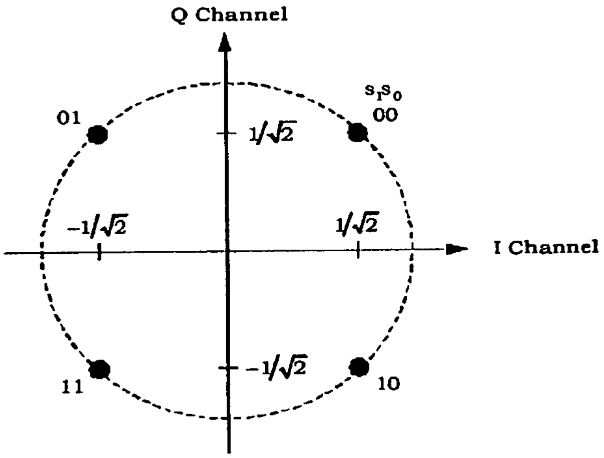


Figure 9.3.1.3.2.3.5.1-1. Signal Constellation for QPSK Modulation

9.3.1.3.2.3.5.2 8-PSK Modulation

For physical layer packet sizes of 3,072 bits, groups of three successive channel interleaver output symbols shall be grouped to form 8-PSK modulation symbols. Each group of three adjacent block interleaver output symbols, x(3i), x(3i + 1), and x(3i + 2), i = 0,..., M – 1 as specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol ($m_I(i)$, $m_Q(i)$) as specified in Table 9.3.1.3.2.3.5.2-1. Figure 9.3.1.3.2.3.5.2-1 shows the signal constellation of the 8-PSK modulator, where $s_0 = x(3k)$, $s_1 = x(3k + 1)$, and $s_2 = x(3k + 2)$.

Table 9.3.1.3.2.3.5.2-1. 8-PSK Modulation Table

Interleaved Symbols			Modulation Symbols	
s_2 x(3k + 2)	s_1 x(3k + 1)	s_0 x(3k)	$m_I(k)$	$m_Q(k)$
0	0	0	C	S
0	0	1	S	C
0	1	1	–S	C
0	1	0	–C	S
1	1	0	–C	–S
1	1	1	–S	–C
1	0	1	S	–C
1	0	0	C	–S

Note: [illegible]239= and [illegible]827π ≈ .

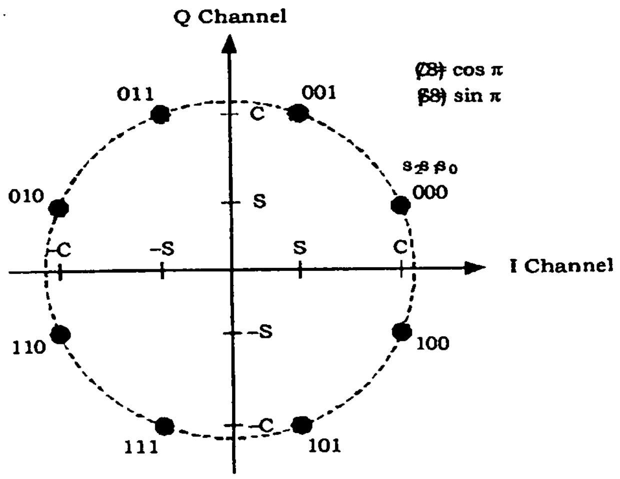


Figure 9.3.1.3.2.3.5.2-1. Signal Constellation for 8-PSK Modulation

9.3.1.3.2.3.5.3 16-QAM Modulation

For physical layer packet sizes of 4,096 bits, groups of four successive channel interleaver output symbols shall be grouped to form 16-QAM modulation symbols. Each group of four adjacent block interleaver output symbols, x(4i), x(4i + 1), x(4i + 2), and x(4i + 3), i = 0,..., M – 1 as specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol ($m_I(i)$, $m_Q(i)$) as specified in Table 9.3.1.3.2.3.5.3-1. Figure 9.3.1.3.2.3.5.3-1 shows the signal constellation of the 16QAM modulator, where s_0 = x(4k), s_1 = x(4k + 1), s_2 = x(4k + 2), and s_3 = x(4k + 3).

Table 9.3.1.3.2.3.5.3-1. 16-QAM Modulation Table

Interleaved Symbols				Modulation Symbols	
s_3 x(4k + 3)	s_2 x(4k + 2)	s_1 x(4k + 1)	s_0 x(4k)	$m_Q(k)$	$m_I(k)$
0	0	0	0	3A	3A
0	0	0	1	3A	A
0	0	1	1	3A	–A
0	0	1	0	3A	–3A
0	1	0	0	A	3A
0	1	0	1	A	A
0	1	1	1	A	–A
0	1	1	0	A	–3A
1	1	0	0	–A	3A
1	1	0	1	–A	A
1	1	1	1	–A	–A
1	1	1	0	–A	–3A
1	0	0	0	–3A	3A
1	0	0	1	–3A	A
1	0	1	1	–3A	–A
1	0	1	0	–3A	–3A

Note: a.31/√62 ≈ .

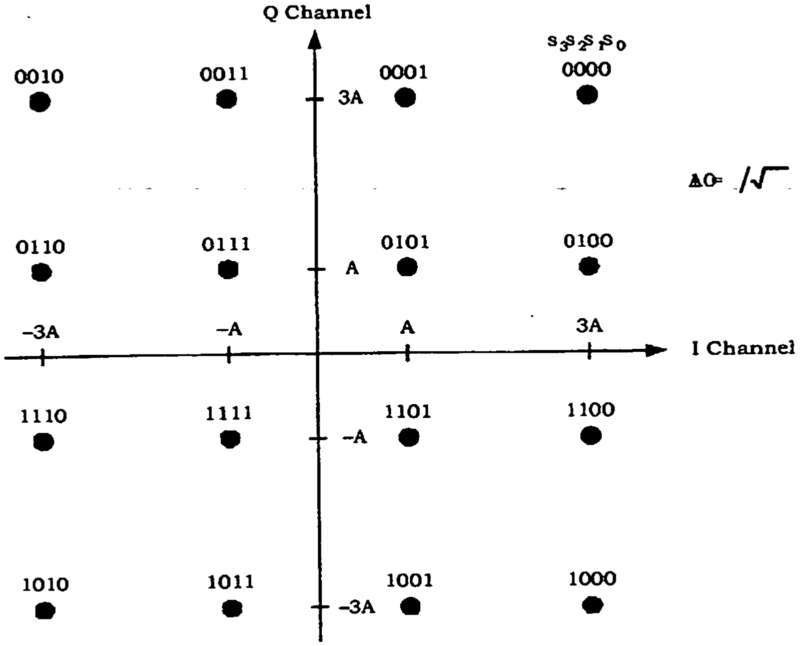


Figure 9.3.1.3.2.3.5.3-1. Signal Constellation for 16-QAM Modulation

9.3.1.3.2.3.6 Sequence Repetition and Symbol Puncturing

Table 9.3.1.3.2.3.6-1 gives the number of modulation symbols that the modulator provides per physical layer packet and the number of modulation symbols needed for the data portion of the allocated slots. If the number of required modulation symbols is more than the number provided, the complete sequence of input modulation symbols shall be repeated as many full-sequence times as possible followed by a partial transmission if necessary. If a partial transmission is needed, the first portion of the input modulation symbol sequence shall be used. If the number of required modulation symbols is less than the number provided, only the first portion of the input modulation symbol sequence shall be used.

The sequence repetition and symbol puncturing parameters shall be as specified in Table 9.3.1.3.2.3.6-1. The entries in the column labeled "Number of Modulation Symbols Needed" are equal to the number of data TDM chips given in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2.

Table 9.3.1.3.2.3.6-1. Sequence Repetition and Symbol Puncturing Parameters

Data Rate (kbps)	Values per Physical Layer Packet						Approximate Coding	
	Number of Slots	Number of Bits	Number of Modulation Symbols Provided	Number of Modulation Symbols Needed	Number of Full Sequence Transmissions	Number of Modulation Symbols in Last Partial Transmission	Code Rate	Repetition Factor
38.4	16	1,024	2,560	24,576	9	1,536	1/5	9.6
76.8	8	1,024	2,560	12,288	4	2,048	1/5	4.8
153.6	4	1,024	2,560	6,144	2	1,024	1/5	2.4
307.2	2	1,024	2,560	3,072	1	512	1/5	1.2
614.4	1	1,024	1,536	1,536	1	0	1/3	1
307.2	4	2,048	3,072	6,272	2	128	1/3	2.04
614.4	2	2,048	3,072	3,136	1	64	1/3	1.02
1,228.8	1	2,048	3,072	1,536	0	1,536	2/3	1
921.6	2	3,072	3,072	3,136	1	64	1/3	1.02
1,843.2	1	3,072	3,072	1,536	0	1,536	2/3	1
1,228.8	2	4,096	3,072	3,136	1	64	1/3	1.02
2,457.6	1	4,096	3,072	1,536	0	1,536	2/3	1

9.3.1.3.2.3.7 Symbol Demultiplexing

The in-phase stream at the output of the sequence repetition operation shall be demultiplexed into 16 parallel streams labeled I_0, I_1, I_2,..., I_{15}. If $m_I(0)$, $m_I(1)$, $m_I(2)$, $m_I(3)$,... denotes the sequence of sequence-repeated modulation output values in the in-phase stream, then for each k = 0, 1, 2,..., 15, the kth demultiplexed stream I_k shall consist of the values $m_I(k)$, $m_I(16 + k)$, $m_I(32 + k)$, $m_I(48 + k)$,....

Similarly, the quadrature stream at the output of the sequence repetition operation shall be demultiplexed into 16 parallel streams labeled Q_0, Q_1, Q_2,..., Q_{15}. If $m_Q(0)$, $m_Q(1)$, $m_Q(2)$, $m_Q(3)$,...denotes the sequence of sequence-repeated modulation output values in the quadrature stream, then for each k = 0, 1, 2,...,15, the kth demultiplexed stream Q_k shall consist of the values $m_Q(k)$, $m_Q(16 + k)$, $m_Q(32 + k)$, $m_Q(48 + k)$,....

Each demultiplexed stream at the output of the symbol demultiplexer shall consist of modulation values at the rate of 76.8 ksps.

9.3.1.3.2.3.8 Walsh Channel Assignment

The individual streams generated by the symbol demultiplexer shall be assigned to one of 16 distinct Walsh channels. For each k = 0, 1, 2,..., 15, the demultiplexed streams with labels I_k and Q_k shall be assigned to the in-phase and quadrature phases, respectively, of the kth Walsh channel W_k^{16}. The modulation values associated with the in-phase and quadrature phase components of the same Walsh channel are referred to as Walsh symbols.

9.3.1.3.2.3.9 Walsh Channel Scaling

The modulated symbols on each branch of each Walsh channel shall be scaled to maintain a constant total transmit power independent of data rate. For this purpose, each orthogonal channel shall be scaled by a gain of $\frac{1}{\sqrt{16}} = \frac{1}{4}$. The gain settings are normalized to a unity reference equivalent to unmodulated BPSK transmitted at full power.

9.3.1.3.2.3.10 Walsh Chip Level Summing

The scaled Walsh chips associated with the 16 Walsh channels shall be summed on a chip-by-chip basis.

9.3.1.3.2.4 Control Channel

The Control Channel transmits broadcast messages and access-terminal-directed messages. The Control Channel messages shall be transmitted at a data rate of 76.8 kbps or 38.4 kbps. The modulation characteristics shall be the same as those of the Forward Traffic Channel at the corresponding data rate. The Control Channel transmissions shall be distinguished from Forward Traffic Channel transmissions by having a preamble that is covered by a bi-orthogonal cover sequence with MACIndex 2 or 3, as specified in 9.3.1.3.2.3.1. A MACIndex value of 2 shall be used for the 76.8-kbps data rate, and a MACIndex value of 3 shall be used for the 38.4-kbps data rate.

9.3.1.3.3 Time-Division Multiplexing

The Forward Traffic Channel or Control Channel data modulation chips shall be time-division multiplexed with the preamble, Pilot Channel, and MAC Channel chips according to the timing diagrams in Figure 9.3.1.3.3-1, Figure 9.3.1.3.3-2, Figure 9.3.1.3.3-3, and Figure 9.3.1.3.3-4. The multiplexing parameters shall be as specified in Table 9.3.1.3.3-1.

The Walsh chip rate shall be fixed at 1.2288 Mcps.

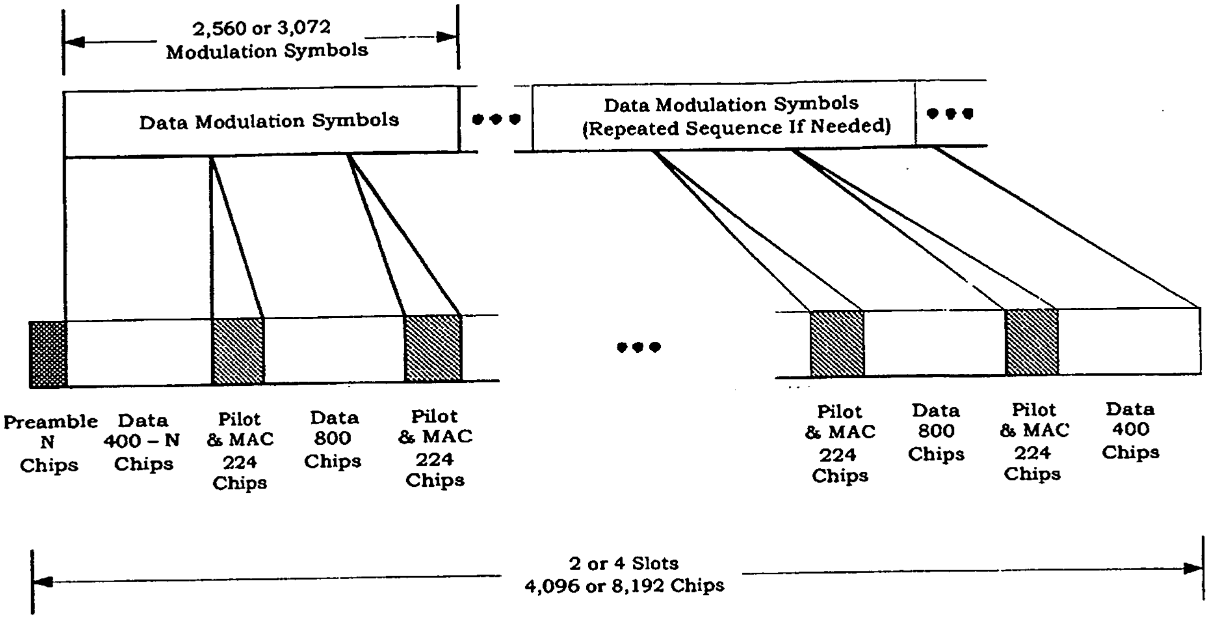


Figure 9.3.1.3.3-1. Preamble, Pilot, MAC, and Data Multiplexing for the Multiple-Slot Cases with Data Rates of 153.6, 307.2, 614.4, 921.6, and 1228.8 kbps

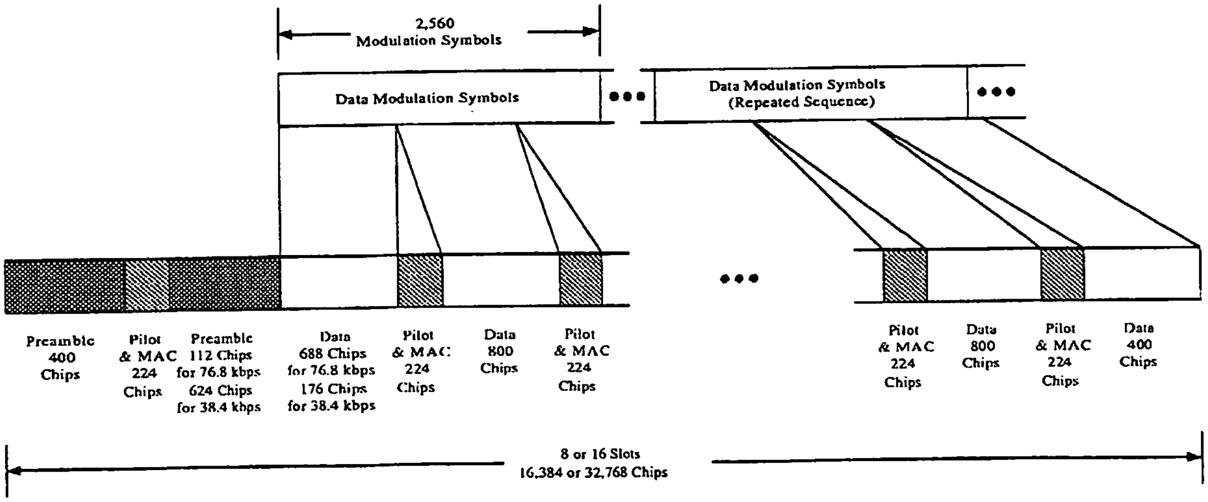


Figure 9.3.1.3.3-2. Preamble, Pilot, MAC, and Data Multiplexing with Data Rates of 38.4 and 76.8 kbps

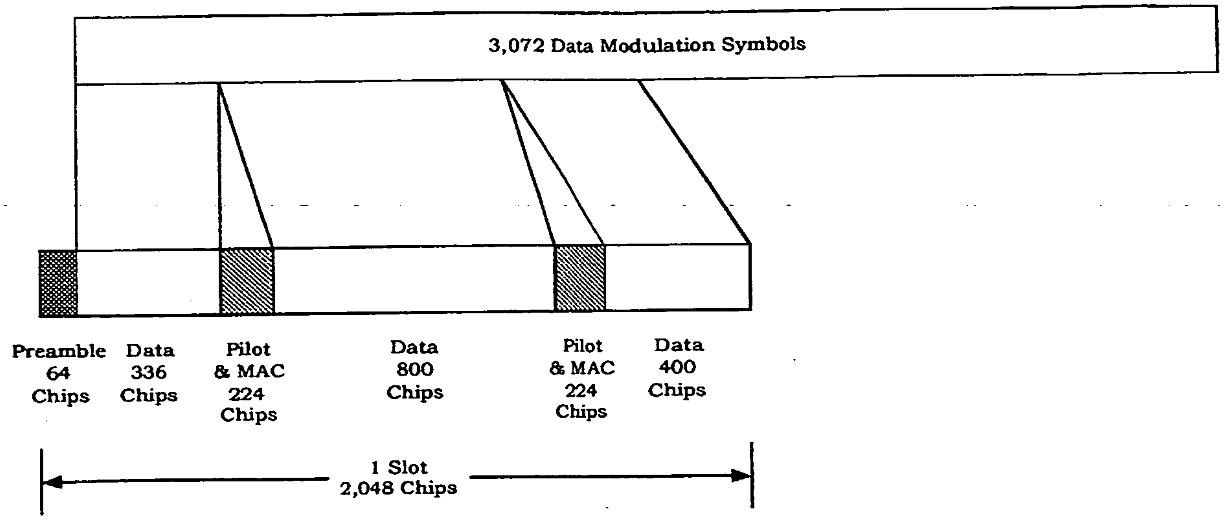


Figure 9.3.1.3.3-3. Preamble, Pilot, MAC, and Data Multiplexing for the 1-Slot Cases with Data Rates of 1.2288, 1.8432, and 2.4576 Mbps

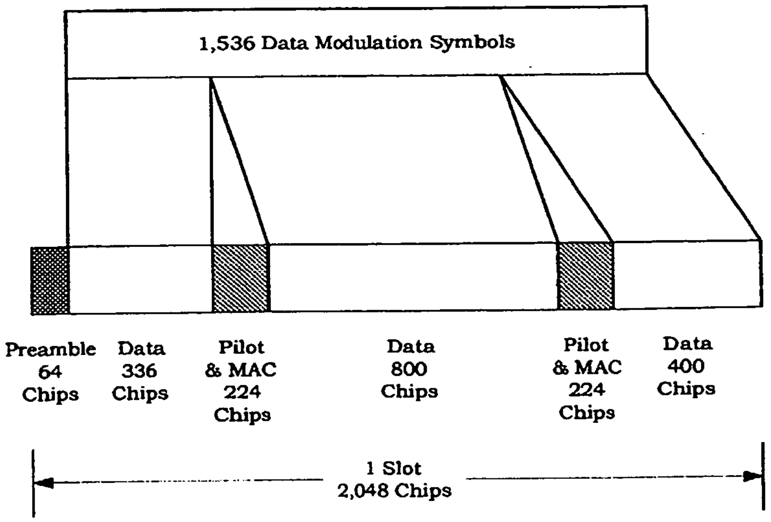


Figure 9.3.1.3.3-4. Preamble, Pilot, MAC, and Data Multiplexing for the 1-Slot Case with a Data Rate of 614.4 kbps

Table 9.3.1.3.3-1. Preamble, Pilot, MAC, and Data Multiplexing Parameters

Data Rate (kbps)	Number of Values per Physical Layer Packet					
	Slots	Bits	Preamble Chips	Pilot Chips	MAC Chips	Data Chips
38.4	16	1,024	1,024	3,072	4,096	24,576
76.8	8	1,024	512	1,536	2,048	12,288
153.6	4	1,024	256	768	1,024	6,144
307.2	2	1,024	128	384	512	3,072
614.4	1	1,024	64	192	256	1,536
307.2	4	2,048	128	768	1,024	6,272
614.4	2	2,048	64	384	512	3,136
1,228.8	1	2,048	64	192	256	1,536
921.6	2	3,072	64	384	512	3,136
1,843.2	1	3,072	64	192	256	1,536
1,228.8	2	4,096	64	384	512	3,136
2,457.6	1	4,096	64	192	256	1,536

9.3.1.3.4 Quadrature Spreading

Following orthogonal spreading, the combined modulation sequence shall be quadrature spread as shown in Figure 9.3.1.3.1-1. The spreading sequence shall be a quadrature sequence of length 2^{15} (i.e., 32768 PN chips in length). This sequence is called the pilot PN sequence and shall be based on the following characteristic polynomials:

$$P_I(x) = x^{15} + x^{10} + x^8 + x^7 + x^6 + x^2 + 1$$

(for the in-phase (I) sequence)

and

$$P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^4 + x^3 + 1$$

(for the quadrature-phase (Q) sequence).

The maximum length linear feedback shift-register sequences {I(n)} and {Q(n)} based on the above polynomials are of length $2^{15} - 1$ and can be generated by the following linear recursions:

$$I(n) = I(n-15) \oplus I(n-13) \oplus I(n-9) \oplus I(n-8) \oplus I(n-7) \oplus I(n-5)$$

(based on $P_I(x)$ as the characteristic polynomial)

and

$$Q(n) = Q(n-15) \oplus Q(n-12) \oplus Q(n-11) \oplus Q(n-10) \oplus Q(n-6) \oplus Q(n-5) \oplus Q(n-4) \oplus Q(n-3)$$

(based on $P_Q(x)$ as the characteristic polynomial),

where I(n) and Q(n) are binary valued ('0' and '1') and the additions are modulo-2. In order to obtain the I and Q pilot PN sequences (of period 2^{15}), a '0' is inserted in the {I(n)} and {Q(n)} sequences after 14 consecutive '0' outputs (this occurs only once in each period). Therefore, the pilot PN sequences have one run of 15 consecutive '0' outputs instead of 14.

The chip rate for the pilot PN sequence shall be 1.2288Mcps. The pilot PN sequence period is 32768/1228800 = 26.666... ms, and exactly 75 pilot PN sequence repetitions occur every 2 seconds.

Pilot Channels shall be identified by an offset index in the range from 0 through 511 inclusive. This offset index shall specify the offset value (in units of 64 chips) of the pilot PN sequence from the zero-offset pilot PN sequence. The zero-offset pilot PN sequence shall be such that the start of the sequence shall be output at the beginning of every even second in time, referenced to access network transmission time. The start of the zero-offset pilot PN sequence for either the I or Q sequences shall be defined as the state of the sequence for which the next 15 outputs inclusive are '0'. Equivalently, the zero-offset sequence is defined such that the last chip prior to the even-second mark as referenced to the transmit time reference is a '1' prior to the 15 consecutive '0's.

9.3.1.3.5 Filtering

9.3.1.3.5.1 Baseband Filtering

Following the quadrature spreading operation, the I' and Q' impulses are applied to the inputs of the I and Q baseband filters as shown in Figure 9.3.1.3.1-1. The baseband filters shall have a frequency response S(f) that satisfies the limits given in Figure 9.3.1.3.5.1-1. Specifically, the normalized frequency response of the filter shall be contained within $\pm\delta_1$ in the passband $0 \le f \le f_p$ and shall be less than or equal to $-\delta_2$ in the stopband $f \ge f_s$. The numerical values for the parameters are δ_1 = 1.5 dB, δ_2 = 40 dB, f_p = 590 kHz, and f_s = 740 kHz.

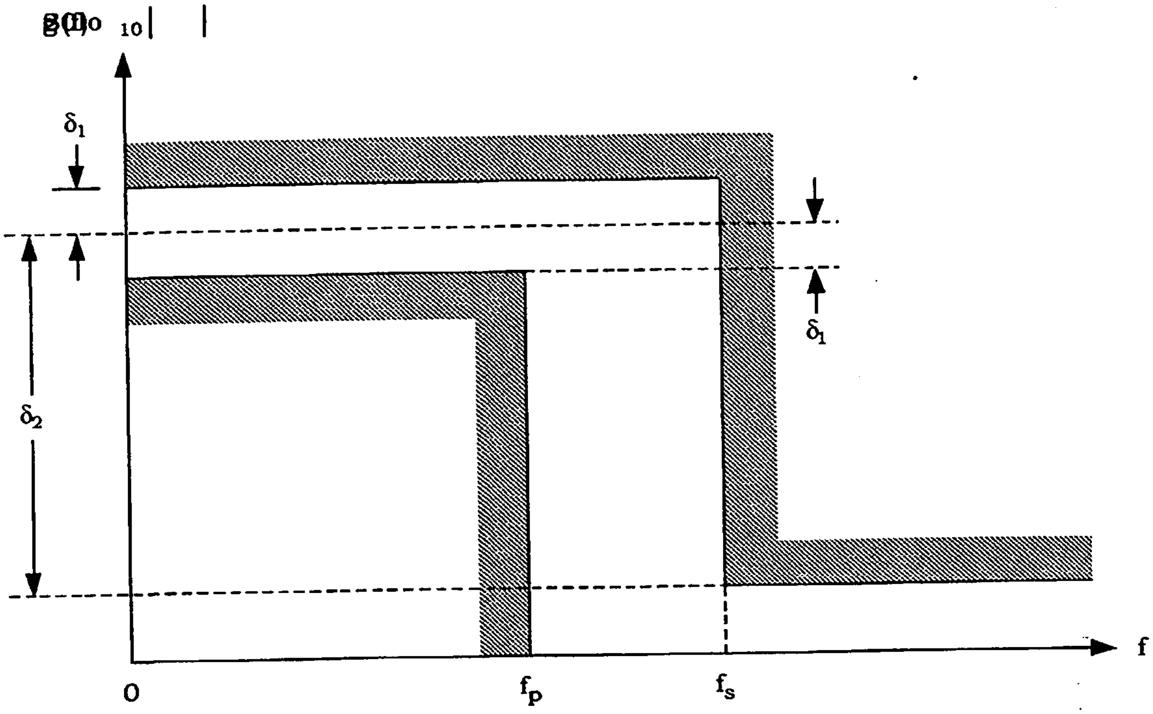


Figure 9.3.1.3.5.1-1. Baseband Filter Frequency Response Limits

The impulse response of the baseband filter, s(t), should satisfy the following equation:

$$\text{Mean Squared Error} = \sum_{k=0}^{\infty} [\alpha s(kT_S - \tau) - h(k)]^2 \leq 0.03,$$

where the constants α and τ are used to minimize the mean squared error. The constant T_S is equal to 203.451... ns, which equals one quarter of a PN chip. The values of the coefficients h(k), for k < 48, are given in Table 9.3.1.3.5.1-1; h(k) = 0 for k ≥ 48. Note that h(k) equals h(47 – k).

Table 9.3.1.3.5.1-1. Baseband Filter Coefficients

k	h(k)
0, 47	–0.025288315
1, 46	–0.034167931
2, 45	–0.035752323
3, 44	–0.016733702
4, 43	0.021602514
5, 42	0.064938487
6, 41	0.091002137
7, 40	0.081894974
8, 39	0.037071157
9, 38	–0.021998074
10, 37	–0.060716277
11, 36	–0.051178658
12, 35	0.007874526
13, 34	0.084368728
14, 33	0.126869306
15, 32	0.094528345
16, 31	–0.012839661
17, 30	–0.143477028
18, 29	–0.211829088
19, 28	–0.140513128
20, 27	0.094601918
21, 26	0.441387140
22, 25	0.785875640
23, 24	1.0

9.3.1.3.5.2 Phase Characteristics

The access network shall provide phase equalization for the transmit signal path.[48] The equalizing filter shall be designed to provide the equivalent baseband transfer function

[48] This equalization simplifies the design of the access terminal receive filters.

$$H(\omega) = K\frac{\omega^2 + j\alpha\omega\omega_0 - \omega_0{}^2}{\omega^2 - j\alpha\omega\omega_0 - \omega_0{}^2},$$

where K is an arbitrary gain, j equals $\sqrt{-1}$, α equals 1.36, ω_0 equals $2\pi \times 3.15 \times 10^5$, and ω is the radian frequency. The equalizing filter implementation shall be equivalent to applying baseband filters with this transfer function, individually, to the baseband I and Q waveforms.

A phase error test filter is defined to be the overall access network transmitter filter (including the equalizing filter) cascaded with a filter having a transfer function that is the inverse of the equalizing filter specified above. The response of the test filter should have a mean squared phase error from the best fit linear phase response that is no greater than 0.01 squared radians when integrated over the frequency range 1 kHz $\leq |f - f_c| \leq$ 630 kHz. For purposes of this requirement, "overall" shall mean from the I and Q baseband filter inputs (see 9.3.1.3.5.1) to the RF output of the transmitter.

9.3.1.3.6 Synchronization and Timing

9.3.1.3.6.1 Timing Reference Source

Each sector shall use a time base reference from which all time-critical transmission components, including pilot PN sequences, slots, and Walsh functions, shall be derived. The time-base reference shall be time-aligned to System Time, as described 1.13. Reliable external means should be provided at each sector to synchronize each sector's time base reference to System Time. Each sector should use a frequency reference of sufficient accuracy to maintain time alignment to System Time. In the event that the external source of System Time is lost,[49] the sector shall maintain transmit timing within ±10 μs of System Time for a period of not less than 8 hours.

9.3.1.3.6.2 Sector Transmission Time

All sectors should radiate the pilot PN sequence within ±3 □s of System Time and shall radiate the pilot PN sequence within ±10 □s of System Time.

Time measurements are made at the sector antenna connector. If a sector has multiple radiating antenna connectors for the same CDMA channel, time measurements are made at the antenna connector having the earliest radiated signal.

The rate of change for timing corrections shall not exceed 102 ns (1/8 PN chip) per 200 ms.

[49] These guidelines on time keeping requirements reflect the fact that the amount of time error between sectors that can be tolerated in an access network is not a hard limit. Each access terminal can search an ever-increasing time window as directed by the sectors. However, increasing this window gradually degrades performance since wider windows require a longer time for the access terminals to search out and locate the various arrivals from all sectors that may be in view.

10 COMMON ALGORITHMS AND DATA STRUCTURES

10.1 Channel Record

The Channel record defines an access network channel frequency and the type of system on that frequency. This record contains the following fields:

Field	Length (bits)
SystemType	8
BandClass	5
ChannelNumber	11

SystemType The access network shall set this field to one of the following values:

Table 10.1-1. SystemType Encoding

Field value	Meaning
0x00	System compliant to this specification
0x01	System compliant to [2][50]
0x02-0xff	Reserved

BandClass The access network shall set this field to the band class number corresponding to the frequency assignment of the channel specified by this record (see 9.2.1.1.1).

ChannelNumber The access network shall set this field to the channel number corresponding to the frequency assignment of the channel specified by this record (see 9.2.1.1.1).

[50] SystemType of 0x01 applies to [2] and all of its predecessors.

10.2 Access Terminal Identifier Record

The Access Terminal Identifier record provides a fully qualified access terminal address. This record contains the following fields:

Field	Length (bits)
ATIType	2
ATI	0 or 32

ATIType Access Terminal Identifier Type. This field shall be set to the type of the ATI, as shown in Table 10.2-1:

Table 10.2-1. ATIType Field Encoding

ATIType	ATIType Description	ATI Length (bits)
'00'	Broadcast ATI (BATI)	0
'01'	Multicast ATI (MATI)	32
'10'	Unicast ATI	32
'11'	Random ATI (RATI)	32

ATI Access Terminal Identifier. The field is included only if ATIType is not equal to '00'. This field shall be set as shown in Table 10.2-1.

10.3 Attribute Record

The attribute record defines a set of suggested values for a given attribute. The attribute record format is defined, such that if the recipient does not recognize the attribute, it can discard it and parse attribute records that follow this record.

An attribute can be one of the following three types:

- Simple attribute, if it contains a single value,
- Attribute list, if it contains multiple single values which are to be interpreted as different suggested values for the same attribute identifier (e.g., a list of possible protocol Subtypes for the same protocol Type), or
- Complex attribute, if it contains multiple values that together form a complex value for a particular attribute identifier (e.g., a set of parameters for the Route Update Protocol).

Simple attributes are a special case of an attribute list containing a single value.

The type of the attribute is determined by the attribute identifier.

The sender of a ConfigurationResponse message (see 10.7) selects an attribute-value from a ConfigurationRequest message by sending the attribute value if it is a simple attribute or a selected value out of an attribute list. Selection of complex-attributes is done by sending the value identifier which identifies the complex value.

The format of a simple attribute and attribute list is given by

Field	Length (bits)
Length	8
AttributeID	Protocol Specific

An appropriate number of instances of the following record

AttributeValue	Attribute dependent

Reserved	variable

Length Length in octets of the attribute record, excluding the Length field.

AttributeID Attribute identifiers are unique in the context of the protocol being configured.

AttributeValue A suggested value for the attribute. Attribute value lengths are, in general, an integer number of octets. Attribute values have an explicit or implicit length indication (e.g., fixed length or null terminated strings) so that the recipient can successfully parse the record when more than one value is provided.

Reserved The length of this field is the smallest value that will make the attribute record octet aligned. The sender shall set this field to zero. The receiver shall ignore this field.

The format of a complex attribute is given by

Field	Length (bits)
Length	8
AttributeID	Protocol Specific
One or more instances of the following fields	
ValueID	Protocol Specific
An appropriate number of instances of the following record for each instance of the ValueID field	
AttributeValue	Attribute dependent
Reserved	variable

Length — Length in octets of the attribute record, excluding the Length field.

AttributeID — Attribute identifiers are unique in the context of the protocol being configured.

ValueID — It identifies the set of attribute values following this field. The sender shall increment this field for each new set of values for this complex attribute.

AttributeValue — A suggested value for the attribute. Attribute value lengths are in general an integer number of octets. Attribute values have an explicit or implicit length indication (e.g., fixed length or null terminated strings) so that the recipient can successfully parse the record when more than one value is provided.

Reserved — The length of this field is the smallest value that will make the attribute record octet aligned. The sender shall set this field to zero. The receiver shall ignore this field.

10.4 Hash Function

The hash function takes three arguments, ***Key*** (typically the access terminal's ATI), ***N*** (the number of resources), and ***Decorrelate*** (an argument used to de-correlate values obtained for different applications for the same access terminal).

Define:

- Word ***L*** to be bits 0-15 of ***Key***
- Word ***H*** to be bits 16-31 of ***Key***

where bit 0 is the least significant bit of ***Key***.

The hash value is computed as follows[51]:

$$R = \lfloor \boldsymbol{N} \times ((40503 \times (\boldsymbol{L} \oplus \boldsymbol{H} \oplus \text{Decorrelate})) \bmod 2^{16}) / 2^{16} \rfloor.$$

10.5 Pseudorandom Number Generator

10.5.1 General Procedures

When an access terminal is required to use the pseudo random number generator described in this section, then the access terminal shall implement the linear congruential generator defined by

$$z_n = a \times z_{n-1} \bmod m$$

where $a = 7^5 = 16807$ and $m = 2^{31} - 1 = 2147483647$. z_n is the output of the generator.[52]

The access terminal shall initialize the random number generator as defined in 10.5.2.

The access terminal shall compute a new z_n for each subsequent use.

The access terminal shall use the value $u_n = z_n / m$ for those applications that require a binary fraction u_n, $0 < u_n < 1$.

The access terminal shall use the value $k_n = \lfloor N \times z_n / m \rfloor$ for those applications that require a small integer k_n, $0 \le k_n \le N-1$.

10.5.2 Initialization

The access terminal shall initialize the random number generator by setting z_0 to

$$z_0 = (\text{HardwareID} \oplus \chi) \bmod m$$

where HardwareID is the least 32 bits of the hardware identifier associated with the access terminal, and χ is a time-varying physical measure available to the access terminal. If the initial value so produced is found to be zero, the access terminal shall repeat the procedure with a different value of χ.

[51] This formula is adapted from Knuth, D. N., *Sorting and Searching*, vol. 3 of *The Art of Computer Programming*, 3 vols., (Reading, MA: Addison-Wesley, 1973), pp. 508-513. The symbol ⊕ represents bitwise exclusive-or function (or modulo 2 addition) and the symbol ⌊ ⌋ represents the "largest integer smaller than" function.

[52] This generator has full period, ranging over all integers from 1 to m-1; the values 0 and m are never produced. Several suitable implementations can be found in Park, Stephen K. and Miller, Keith W., "Random Number Generators: Good Ones are Hard to Find," *Communications of the ACM*, vol. 31, no. 10, October 1988, pp. 1192-1201.

10.6 Sequence Number Validation

When the order in which protocol messages are delivered is important, air interface protocols use a sequence number to verify this order.

The sequence number has ***s*** bits.The sequence space is 2^s. All operations and comparisons performed on sequence numbers shall be carried out in unsigned modulo 2^s arithmetic. For any message sequence number ***N***, the sequence numbers in the range [N+1, N+2^{s-1} -1] shall be considered greater than ***N***, and the sequence numbers in the range [N-2^{s-1}, N-1] shall be considered smaller than ***N***.

The receiver of the message maintains a receive pointer ***V(R)*** whose initialization is defined as part of the protocol. When a message arrives, the receiver compares the sequence number of the message with ***V(R)***. If the sequence number is greater than ***V(R)***, the message is considered a valid message and ***V(R)*** is set to this sequence number; otherwise, the message is considered a stale message.

10.7 Generic Configuration Protocol

10.7.1 Introduction

The Generic Configuration Protocol provides a means to negotiate protocol parameters. The procedure procedure consists of the initiator sending an attribute and one or more allowed values. The responder then selects one of the offered values. Each attribute must have a well known default value; if the responder does not select any of the offered values, the default value is selected.

10.7.2 Procedures

10.7.2.1 Configuration Negotiation

The protocol uses a ConfigurationRequest message and a ConfigurationResponse message to negotiate a mutually acceptable configuration. The initiator uses the ConfigurationRequest message to provide the responder with a list of acceptable attribute values for each attribute. The responder uses the ConfigurationResponse message to provide the initiator with the accepted attribute value for each attribute, choosing the accepted attribute value from the initiator's acceptable attribute value list.

The initiator orders the acceptable attribute values for each attribute in descending order of preference. The initiator sends these ordered attribute-value lists to the responder using one or more ConfigurationRequest messages. If the ordered attribute value lists fit within one ConfigurationRequest message, then the initiator should use one ConfigurationRequest message. If the ordered attribute value lists do not fit within one ConfigurationRequest message, then the initiator may use more than one ConfigurationRequest message. Each ConfigurationRequest message shall contain one or more complete ordered attribute value lists; an ordered attribute value list for an attribute shall not be split within a ConfigurationRequest message and shall not be split across multiple ConfigurationRequest messages.

After sending a ConfiguratioRequest message, the sender shall set the value of all parameters that were listed in the message to NULL.

After receiving a ConfigurationRequest message, the responder shall respond within $T_{Turnaround}$, where $T_{Turnaround}$ = 2 seconds, unless specified otherwise. For each attribute included in the ConfigurationRequest message, the responder chooses an acceptable attribute value from the associated acceptable attribute value list. If the responder does not recognize an attribute or does not find an acceptable attribute value in the associated attribute list, then the attribute is skipped. The responder sends the accepted attribute value for each attribute within one ConfigurationResponse message. The responder shall list the attributes in the ConfigurationResponse message in the order they were listed in the ConfigurationRequest message. In addition, the value included for each attribute shall be one of the values listed in the ConfigurationRequest message. After receiving ConfigurationResponse message, the initiator pairs the received message with the associated ConfigurationRequest message. If the ConfigurationResponse message does not contain an attribute found in the associated ConfigurationRequest message, then the initiator shall assume that the missing attribute is using the default value.

If the initiator requires no further negotiation of protocols or configuration of negotiated protocols and if the value of the any of the parameters for which the initiator has sent a ConfigurationRequest message is NULL, then the sender shall declare a failure.

The initiator and the responder shall use the attribute values in the ConfigurationResponse messages as the configured attribute values, provided that the attribute values were also present in the associated ConfigurationRequest message.

10.7.3 Message Formats

The receiver shall discard all unrecognized messages. The receiver shall discard all unrecognized fields following the fields defined herein. The receiver may log the message for diagnostic reasons.

The specification of the Physical Layer channels on which the following messages are to be carried; and, whether the messages are to be sent reliably or as best-effort, is provided in the context of the protocols in which these messages are used.

10.7.3.1 ConfigurationRequest

The sender sends the ConfigurationRequest message to offer a set of attribute-values for a given attribute.

Field	Length (bits)
MessageID	Protocol dependent
TransactionID	8

Zero or more instances of the following record

AttributeRecord	Attribute dependent

MessageID The value of this field is specified in the context of the protocol using this message. The value 0x50 is recommended.

TransactionID The sender shall increment this value for each new ConfigurationRequest message sent.

AttributeRecord The format of this record is specified in 10.3.

10.7.3.2 ConfigurationResponse

The sender sends a ConfigurationResponse message to select an attribute-value from a list of offered values.

Field	Length (bits)
MessageID	Protocol dependent
TransactionID	8

Zero or more instances of the following record

AttributeRecord	Attribute dependent

MessageID The value of this field is specified in the context of the protocol using this message. The value 0x51 is recommended.

TransactionID The sender shall set this value to the TransactionID field of the corresponding ConfigurationRequest message.

AttributeRecord An attribute record containing a single attribute value. If this message selects a complex attribute, only the ValueID field of the complex attribute shall be include in the message. The format of the AttributeRecord is given in 10.3. The sender shall not include more than one attribute record with the same attribute identifier.

No text.

11 ASSIGNED NAMES AND NUMBERS

11.1 Protocols

Protocol Type		Protocol Subtype		Page
Name	ID	Name	ID	
Physical Layer	0x00	Default Physical Layer	0x0000	9-1
Control Channel MAC	0x01	Default Control Channel MAC	0x0000	8-5
Access Channel MAC	0x02	Default Access Channel MAC	0x0000	8-13
Forward Traffic Channel MAC	0x03	Default Forward Traffic Channel MAC	0x0000	8-29
Reverse Traffic Channel MAC	0x04	Default Reverse Traffic Channel MAC	0x0000	8-42
Key Exchange	0x05	Default Key Exchange	0x0000	7-9
Key Exchange	0x05	DH Key Exchange	0x0001	7-10
Authentication	0x06	Default Authentication	0x0000	7-24
Authentication	0x06	SHA-1 Authentication	0x0001	7-25
Encryption	0x07	Default Encryption	0x0000	7-29
Security	0x08	Default Security	0x0000	7-6
Security	0x08	Generic Security	0x0001	7-7
Packet Consolidation	0x09	Default Packet Consolidation	0x0000	6-75
Air-Link Management	0x0a	Default Air-Link Management	0x0000	6-5
Initialization State	0x0b	Default Initialization State	0x0000	6-15
Idle State	0x0c	Default Idle State	0x0000	6-20
Connected State	0x0d	Default Connected State	0x0000	6-33
Route Update	0x0e	Default Route Update	0x0000	6-39
Overhead Messages	0x0f	N/A	N/A	6-82
Session Management	0x10	Default Session Management	0x0000	5-2
Address Management	0x11	Default Address Management	0x0000	5-14
Session Configuration	0x12	Default Session Configuration	0x0000	5-28
Stream	0x13	Default Stream	0x0000	4-1
Stream 0 Application	0x14	Default Signaling Application	0x0000	2-1
Stream 1 Application	0x15	Default Packet Application bound to	0x0001	3-1

Protocol Type		Protocol Subtype		Page
Name	ID	Name	ID	
		the access network.		
Stream 1 Application	0x15	Default Packet Application bound to the service network	0x0002	3-1
Stream 2 Application	0x16	Default Packet Application bound to the access network	0x0001	3-1
Stream 2 Application	0x16	Default Packet Application bound to the service network	0x0002	3-1
Stream 3 Application	0x17	Default Packet Application bound to the access network	0x0001	3-1
Stream 3 Application	0x17	Default Packet Application bound to the service network	0x0002	3-1

11.2 Messages

Protocol / Application		Message		Page
Subtype Name	Type ID	Name	ID	
Default Access Channel MAC	0x02	ACAck	0x00	8-23
Default Access Channel MAC	0x02	AccessParameters	0x01	8-23
DH Key Exchange	0x05	ANKeyComplete	0x02	7-17
DH Key Exchange	0x05	ATKeyComplete	0x03	7-18
Default Reverse Traffic Channel MAC	0x04	BroadcastReverseRateLimit	0x01	8-49
Default Session Configuration	0x12	ConfigurationComplete	0x00	5-34
Default Access Channel MAC	0x02	ConfigurationRequest	0x50	8-27
Default Forward Traffic Channel MAC	0x03	ConfigurationRequest	0x50	8-39
Default Idle State	0x0c	ConfigurationRequest	0x50	6-31
Default Packet	0x15 – 0x17	ConfigurationRequest	0x50	3-5
Default Reverse Traffic Channel MAC	0x04	ConfigurationRequest	0x50	8-56
Default Route Update	0x0e	ConfigurationRequest	0x50	6-65
Default Session Configuration	0x12	ConfigurationRequest	0x50	5-37
Default Session Management	0x10	ConfigurationRequest	0x50	5-12
Default Stream	0x13	ConfigurationRequest	0x50	4-3
DH Key Exchange	0x05	ConfigurationRequest	0x50	7-19
SHA-1 Authentication	0x06	ConfigurationRequest	0x50	7-28
Default Access Channel MAC	0x02	ConfigurationResponse	0x51	8-27
Default Forward Traffic Channel MAC	0x03	ConfigurationResponse	0x51	8-40
Default Idle State	0x0c	ConfigurationResponse	0x51	6-31
Default Packet	0x15 – 0x17	ConfigurationResponse	0x51	3-2
Default Reverse Traffic Channel MAC	0x04	ConfigurationResponse	0x51	8-56
Default Route Update	0x0e	ConfigurationResponse	0x51	6-73
Default Session Configuration	0x12	ConfigurationResponse	0x51	5-37

Protocol / Application		Message		Page
Subtype Name	Type ID	Name	ID	
Default Session Management	0x10	ConfigurationResponse	0x51	5-12
Default Stream	0x13	ConfigurationResponse	0x51	4-5
DH Key Exchange	0x05	ConfigurationResponse	0x51	7-19
SHA-1 Authentication	0x06	ConfigurationResponse	0x51	7-28
Default Session Configuration	0x12	ConfigurationStart	0x04	5-35
Default Connected State	0x0d	ConnectionClose	0x00	6-37
Default Idle State	0x0c	ConnectionDeny	0x02	6-29
Default Idle State	0x0c	ConnectionRequest	0x01	6-28
Default Packet	0x15 – 0x17	DataReady	0x0b	3-4
Default Packet	0x15 – 0x17	DataReadyAck	0x0c	3-5
Default Forward Traffic Channel MAC	0x03	FixedModeRequest	0x00	8-37
Default Forward Traffic Channel MAC	0x03	FixedModeResponse	0x01	8-37
Default Address Management	0x11	HardwareIDRequest	0x03	5-25
Default Address Management	0x11	HardwareIDResponse	0x04	5-25
Default Session Management	0x10	KeepAliveRequest	0x02	5-10
Default Session Management	0x10	KeepAliveResponse	0x03	5-11
DH Key Exchange	0x05	KeyRequest	0x00	7-15
DH Key Exchange	0x05	KeyResponse	0x01	7-16
Default Packet	0x15 – 0x17	LocationAssignment	0x05	3-12
Default Packet	0x15 – 0x17	LocationComplete	0x06	3-14
Default Packet	0x15 – 0x17	LocationRequest	0x03	3-11
Default Packet	0x15 – 0x17	LocationResponse	0x04	3-11
Default Packet	0x15 – 0x17	Nak	0x02	3-7
Default Route Update	0x0e	NeighborList	0x04	6-62
Default Idle State	0x0c	Page	0x00	6-28
Overhead Messages	0x0f	QuickConfig	0x00	6-85
Default Air-Link Management	0x0a	Redirect	0x00	6-12

Protocol / Application		Message		Page
Subtype Name	Type ID	Name	ID	
Default Packet	0x15 – 0x17	Reset	0x00	3-7
Default Signaling	0x14	Reset	0x00	2-16
Default Packet	0x15 – 0x17	ResetAck	0x01	3-7
Default Signaling	0x14	ResetAck	0x01	2-17
Default Route Update	0x0e	ResetReport	0x03	6-61
Default Route Update	0x0e	RouteUpdate	0x00	6-56
Default Reverse Traffic Channel MAC	0x04	RTCAck	0x00	8-48
Overhead Messages	0x0f	SectorParameters	0x01	6-87
Default Session Management	0x10	SessionClose	0x01	5-9
Default Initialization State	0x0b	Sync	‘00’	6-18
Default Route Update	0x0e	TrafficChannelAssignment	0x01	6-58
Default Route Update	0x0e	TrafficChannelComplete	0x02	6-61
Default Address Management	0x11	UATIAssignment	0x01	5-23
Default Address Management	0x11	UATIComplete	0x02	5-24
Default Address Management	0x11	UATIRequest	0x00	5-22
Default Reverse Traffic Channel MAC	0x04	UnicastReverseRateLimit	0x02	8-50
Default Packet	0x15 – 0x17	XoffRequest	0x09	3-4
Default Packet	0x15 – 0x17	XoffResponse	0x0a	3-4
Default Packet	0x15 – 0x17	XonRequest	0x07	3-3
Default Packet	0x15 – 0x17	XonResponse	0x08	3-3